Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001232

International filing date: 28 January 2005 (28.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-019461
Filing date: 28 January 2004 (28.01.2004)

Date of receipt at the International Bureau: 24 March 2005 (24.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP2005/001232

01.2.2005

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

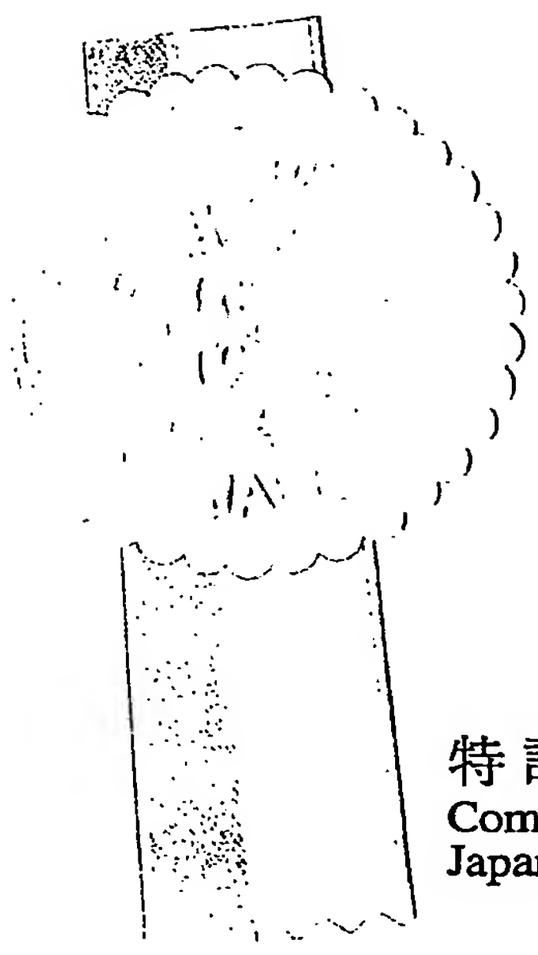
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　１月２８日

出願番号
Application Number: 特願２００４－０１９４６１

[ST. 10/C]: ［Ｊ Ｐ ２００４－０１９４６１］

出願人
Applicant(s): 松下電器産業株式会社



２００５年　３月　９日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０１９９８６

【書類名】　特許願
【整理番号】　7048050059
【提出日】　平成16年 1月28日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G06F 13/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大島　京子
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100099254
　【弁理士】
　【氏名又は名称】　役　昌明
【選任した代理人】
　【識別番号】　100100918
　【弁理士】
　【氏名又は名称】　大橋　公治
【選任した代理人】
　【識別番号】　100105485
　【弁理士】
　【氏名又は名称】　平野　雅典
【選任した代理人】
　【識別番号】　100108729
　【弁理士】
　【氏名又は名称】　林　紘樹
【手数料の表示】
　【予納台帳番号】　037419
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【包括委任状番号】　9102150
【包括委任状番号】　9116348
【包括委任状番号】　9600935
【包括委任状番号】　9700485

【書類名】特許請求の範囲
【請求項１】
ゲート機器に対して認証処理を行う認証手段と、
端末にインストールする端末アプリケーションと、
前記認証手段がゲート機器との認証に成功した場合に、前記ゲート機器から指定された端末アプリケーションを端末にインストールする制御手段と
を備えることを特徴とするセキュアデバイス。
【請求項２】
ゲート機器と端末アプリケーションとの対応関係が規定された対応情報を保持し、前記制御手段は、ゲート機器から指定された端末アプリケーションと前記ゲート機器との関係が前記対応情報に合致する場合にのみ、前記端末アプリケーションを端末にインストールすることを特徴とする請求項１に記載のセキュアデバイス。
【請求項３】
ゲート機器に対して認証処理を行う認証手段と、
カードアプリケーションと
を備え、前記認証手段がゲート機器との認証に成功した場合に、前記ゲート機器から指定されたカードアプリケーションが、端末の端末アプリケーションのアクセスを許容することを特徴とするセキュアデバイス。
【請求項４】
前記認証手段が認証に成功したゲート機器と前記ゲート機器から指定されたカードアプリケーションとの関係を記録するデータベースを保持し、カードアプリケーションは、端末アプリケーションからアクセス要求が有ったときに、前記データベースの情報に基づいて、アクセスの諾否を決定することを特徴とする請求項３に記載のセキュアデバイス。
【請求項５】
ゲート機器に対して認証処理を行い、認証に成功したゲート機器の識別情報を登録する認証手段と、
前記認証手段がゲート機器との認証に成功したことを条件に所定の動作を行う機器に対して、前記機器の検証に供するためにゲート機器の前記識別情報を送信し、または、前記機器に代わって前記識別情報を検証するカードアプリケーションと
を備えることを特徴とするセキュアデバイス。
【請求項６】
前記カードアプリケーションは、前記機器の検証に供するために、入力されたユーザ識別情報を前記機器に送信し、または、前記機器に代わって前記ユーザ識別情報を検証することを特徴とする請求項５に記載のセキュアデバイス。
【請求項７】
セキュアデバイスまたは前記セキュアデバイスを保持する端末との通信手段と、
前記通信手段を通じて前記セキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリケーションを指定するゲートアプリケーションと
を備えることを特徴とするゲート機器。
【請求項８】
セキュアデバイスまたは前記セキュアデバイスを保持する端末との通信手段と、
前記通信手段を通じて前記セキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末の端末アプリケーションがアクセスできるカードアプリケーションを指定するゲートアプリケーションと
を備えることを特徴とするゲート機器。
【請求項９】
セキュアデバイスを保持し、ゲート機器との認証に成功した前記セキュアデバイスから、前記ゲート機器が指定した端末アプリケーションをインストールすることを特徴とする端末装置。

【請求項１０】
セキュアデバイスを保持し、ゲート機器との認証に成功した前記セキュアデバイスが保持するカードアプリケーションの中で、前記ゲート機器が指定したカードアプリケーションにアクセスする端末アプリケーションを備えることを特徴とする端末装置。
【請求項１１】
前記セキュアデバイスが、着脱可能な状態で装着されていることを特徴とする請求項９または請求項１０に記載の端末装置。
【請求項１２】
前記セキュアデバイスが、一体的に埋め込まれていることを特徴とする請求項９または請求項１０に記載の端末装置。
【請求項１３】
ゲート機器との認証に成功したセキュアデバイスから前記ゲート機器の識別情報を取得し、前記識別情報の検証に成功した場合に所定の動作を行うことを特徴とする機器。
【請求項１４】
ゲート機器との認証に成功したセキュアデバイスから前記ゲート機器の識別情報の検証に成功した旨の情報を取得した場合に所定の動作を行うことを特徴とする機器。

【書類名】明細書
【発明の名称】場所限定サービスを行うセキュアデバイスと装置
【技術分野】
【０００１】
本発明は、ＩＣカード等のセキュアデバイスと、このセキュアデバイスとの間で接触通信または非接触通信を行う装置に関し、セキュアデバイスの機能を特定の場所でのみ可能にするものである。
【背景技術】
【０００２】
近年、ＩＣカードは、電子決済用カードや定期乗車券、イベント用チケット、クレジットカード等として広く利用されている。最近では、微細化技術の向上とも相俟って、比較的大容量の記憶空間を持つＩＣカードが作られており、このようなＩＣカードは、カードサービスを実行する複数のカードアプリケーション（以下、アプリケーションを「アプリ」と略称する）を格納することにより、一枚で複数の用途に対応するマルチアプリカードとして使用することができる。
【０００３】
ＩＣカードの通信方式には、ＩＣカードの電気的接点にリーダ・ライタを接触して記録情報の読み書きを行う接触通信と、無線通信で情報をやり取りし、リーダ・ライタとの物理的な接触を必要としない非接触通信との二通りがある。最近は、接触通信及び非接触通信の両方が可能なＩＣカード（コンビカード）を携帯端末装置に搭載し、この携帯端末を電子財布や定期券の替わりに使用することも行われている。
【０００４】
下記特許文献１には、搭載したマルチアプリカードから、目的のカード機能を迅速かつ簡単に選択することを可能にした携帯端末装置が開示されている。この装置を使用するユーザは、マルチアプリカードのカード機能を携帯端末の表示画面に一覧表示して、その中から親アプリと、親アプリに関連付けたアプリ（優先アプリ）とを登録し、マルチアプリカードに記憶させる。例えば、親アプリとして定期乗車券機能を登録し、その優先アプリとして電子マネー機能を登録すると、携帯端末を自動改札装置に翳し、マルチアプリカードの定期乗車券機能を用いて駅構内に入場した場合に、携帯端末の表示画面には、優先アプリの電子マネー機能の表示順位を最上位に設定したアプリ選択画面が表示される。
【０００５】
また、ユーザがマルチアプリカードのアプリ機能を使用すると、その位置が携帯端末のＧＰＳ受信機等の現在位置検出手段で検出されて、使用したアプリ機能と使用位置との関係が携帯端末で記憶される。そして、その位置付近を再び訪れたとき、携帯端末の表示画面には、その位置に対応するアプリ機能の表示順位を最上位に設定したアプリ選択画面が表示される。
【特許文献１】特開２００３－７６９５８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
このように、場所と対応付けてアプリ選択画面の表示を変更することは前記特許文献１に記載されているが、ＩＣカードのカード機能を場所によって限定する発想は、この文献には示されていない。ＩＣカードのカード機能を場所で限定することができるならば、例えば、ＩＣカードを搭載した携帯電話を、社内エリアでは内線電話として使用できるようにし、あるいは、ＩＣカードに格納された特定データを社内エリアでのみ利用できるようにする等、新たな応用が可能になる。
【０００７】
また、ＩＣカードのカード機能を場所によって限定する場合に、前記特許文献１のように、ユーザの登録操作を必要とするのでは、ユーザの処理負担が大きいし、また、携帯端末が位置情報の取得手段を持つ必要があるのでは、携帯端末のコストが高くなる。

【０００８】
本発明は、こうした従来の課題を解決するものであり、ユーザの処理負担やコスト負担を招かずに、カードアプリ機能や装置機能等が発現されるエリアを限定することができるＩＣカード等のセキュアデバイスを提供し、また、このセキュアデバイスと連携して処理を行う装置を提供することを目的としている。
【課題を解決するための手段】
【０００９】
本発明では、セキュアデバイスに、ゲート機器に対して認証処理を行う認証手段と、端末にインストールする端末アプリと、認証手段がゲート機器との認証に成功した場合に、ゲート機器から指定された端末アプリを端末にインストールする制御手段とを設けている。
そのため、セキュアデバイスをゲート機器に翳し、正常に通過したエリアでのみ、端末アプリが端末にインストールされる。ゲート機器のゲートアプリが特定の領域で機能するアプリを指定するので、ユーザの登録操作等は不要であり、また、端末へのＧＰＳ受信機等の装備も必要がない。
【００１０】
また、本発明では、セキュアデバイスに、ゲート機器に対して認証処理を行う認証手段と、カードアプリとを設け、認証手段がゲート機器との認証に成功した場合に、ゲート機器から指定されたカードアプリが、端末の端末アプリのアクセスを許容するようにしている。
そのため、セキュアデバイスをゲート機器に翳し、正常に通過したエリアでのみ、端末アプリは、カードアプリの利用が可能になる。
【００１１】
また、本発明では、セキュアデバイスに、ゲート機器に対して認証処理を行い、認証に成功したゲート機器の識別情報を登録する認証手段と、認証手段がゲート機器との認証に成功したことを条件に所定の動作を行う機器に対して、この機器の検証に供するためにゲート機器の識別情報を送信し、または、この機器に代わって識別情報を検証するカードアプリとを設けている。
そのため、ゲート機器が設置された正規の入口から入場しないと、機器は動作しない。
【００１２】
また、本発明では、ゲート機器に、セキュアデバイスまたはセキュアデバイスを保持する端末との通信手段と、通信手段を通じてセキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリを指定するゲートアプリとを設けている。
また、ゲート機器に、セキュアデバイスまたはセキュアデバイスを保持する端末との通信手段と、通信手段を通じてセキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末の端末アプリがアクセスできるカードアプリを指定するゲートアプリとを設けている。
そのため、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリや、端末アプリがアクセス可能となるカードアプリを指定することができる。
【００１３】
また、本発明の端末装置は、セキュアデバイスを保持し、ゲート機器との認証に成功したセキュアデバイスから、ゲート機器が指定した端末アプリをインストールするように構成している。
また、端末装置は、セキュアデバイスを保持し、ゲート機器との認証に成功したセキュアデバイスが保持するカードアプリの中で、ゲート機器が指定したカードアプリにアクセスする端末アプリを備えている。
そのため、入口にゲート機器が設置された特定のエリアの中でのみ、端末装置の特殊な機能が発揮できる。
【００１４】

また、本発明では、機器が、ゲート機器との認証に成功したセキュアデバイスからゲート機器の識別情報を取得し、この識別情報の検証に成功した場合に所定の動作を行うように構成している。

また、機器が、ゲート機器との認証に成功したセキュアデバイスからゲート機器の識別情報の検証に成功した旨の情報を取得した場合に所定の動作を行うように構成している。

そのため、ユーザがセキュアデバイスを所持して正規の入口から入場しないと、機器は動作しない。

【発明の効果】

【００１５】

本発明のセキュアデバイス、ゲート機器、端末装置及び機器は、連携して、セキュアデバイスのカード機能や、端末装置あるいは機器の機能を、場所と関連付けて変更することができる。例えば、端末装置の機能をオフィスの中と外とで切替えたり、特定の処理機能を限定したエリアでのみ可能にしたり、特定の入口から入場しなければ、部屋の扉や金庫が開かないようにしたりすることができる。

また、こうした処理を、ユーザの処理負担やコスト負担を招かずに実現することができる。

【発明を実施するための最良の形態】

【００１６】

（第１の実施形態）

本発明の第１の実施形態では、ＩＣカードが特定エリアに位置するときだけ、ＩＣカードに格納された端末アプリが、端末にインストールされる場合について説明する。

この特定エリアの入口にはゲートが在り、ゲートアプリは、ＩＣカードとの認証処理に成功すると、ＩＣカードに対して、端末に設定すべき端末アプリを指定する。これを受けて、ＩＣカードは、適宜の時期に、保持する端末アプリの中から、指定された端末アプリを端末にインストールする。

【００１７】

図１は、端末（機器１）が携帯電話１０であり、ＩＣカード（機器２）が、携帯電話１０に装着されたチップ状のコンビカード２０である場合の、携帯電話１０、コンビカード２０及びゲート４０（機器３）の構成について示している。

ゲート４０は、コンビカード２０に対して認証処理や端末アプリの指定を行うゲートアプリ４３と、コンビカード２０への非接触通信を行う非接触通信手段（４）４１と、ゲート４０の動作を制御するＣＰＵ４２とを備えている。

コンビカード２０は、ゲート４０への非接触通信を行う非接触通信手段（３）２２と、携帯電話１０への接触通信を行う接触通信手段（２）２１と、認証情報等が格納された認証情報データベース（ＤＢ）２５と、他の機器１、３との認証処理を行う認証アプリ２４と、携帯電話１０にインストールする端末アプリ２７や設定命令、あるいはそれらのセット２６と、コンビカード２０の動作を制御するＣＰＵ２３とを備えている。

また、携帯電話１０は、コンビカード２０への接触通信を行う接触通信手段（１）１１と、携帯電話１０の動作を制御するＣＰＵ１２とを備えている。

【００１８】

このコンビカード２０の認証情報ＤＢ２５には、図２に示すように、ゲートアプリ４３のＩＤと対応付けて、認証処理に使用する共通鍵や秘密鍵等の認証情報と、携帯電話１０へのインストールが可能な端末アプリ２７のＩＤや、携帯電話１０で設定すべき端末アプリを指定する設定命令のＩＤが格納されている。

【００１９】

設定命令は、例えば、携帯電話１０に対する次のような指示である。

・表示画面の背景イメージに会社ロゴを設定する。
・音（着信時、アプリ実行時）に会社用の音を設定する。
・メインメニューに、社内で使用するイントラネットアプリを追加する。
・デフォルトを内線電話に変更する（外線への発信を０発信に変更）。

また、携帯電話１０へのインストールが可能な端末アプリは、携帯電話１０で保持されていない、設定命令の実行に必要なアプリであり、例えば、設定命令に基づく表示を実行するブラウザ等のソフトウエアである。

【００２０】

図３は、このゲート４０、コンビカード２０及び携帯電話１０が連携して行う処理のシーケンスを示している。

ユーザは、所定エリアに入場する際に、コンビカード２０を装着した携帯電話１０をゲート４０に翳す。ゲート４０のＣＰＵ４２は、非接触通信手段４１の通信圏内にコンビカード２０が進入すると、コンビカード２０に認証アプリＩＤとゲートアプリＩＤとを指定して認証処理を要求する（１－１）。これを受けてコンビカード２０のＣＰＵ２３は認証アプリ２４を起動し、認証アプリ２４は、認証情報ＤＢ２５のゲートアプリＩＤに対応する認証情報を用いて、ゲートアプリ４３との間で、一般的なチャレンジレスポンスによる認証処理を実行する（１－２）。認証処理に成功すると、ゲートアプリ４３は、端末アプリＩＤを指定して、その端末アプリの端末へのインストールを要求する（１－３）。指定する端末アプリＩＤは複数であっても良い。

【００２１】

この要求を受けたコンビカード２０の認証アプリ２４は、認証情報ＤＢ２５の情報から、その端末アプリがインストール可能であることを確認（検証）し、その旨をＣＰＵ２３に伝える。ＣＰＵ２３は、携帯電話１０に端末アプリＩＤを示してインストール要求を送り（２－１）、認証アプリ２４に携帯電話１０との認証処理を行わせる（２－２）。なお、コンビカード２０を携帯電話１０に装着した時点で両者間の認証処理が既に済んでいれば、この認証処理を省略しても良い。認証処理に成功すると、ＣＰＵ２３は、該当する端末アプリ２６、２７を携帯電話１０に送信し（２－３）、携帯電話１０のＣＰＵ１２は、その端末アプリをインストールする。

【００２２】

このように、このゲート４０、コンビカード２０及び携帯電話１０の間では、三者の連携により、コンビカード２０とゲート４０との認証の成功を条件に、コンビカード２０から携帯電話１０への端末アプリのインストールが実行される。そのため、このコンビカード２０の動作や、携帯電話１０の端末アプリを利用する処理は、ゲート４０を通過して入場したエリアでのみ可能になる。

【００２３】

なお、ＩＣカードの国際標準規格（接触通信に関するＩＳＯ７８１６、非接触通信に関するＩＳＯ１４４４３）では、ＩＣカードのカードアプリとリーダ・ライタ側の端末アプリとのデータのやり取りは、端末アプリからカードアプリに送られる「コマンド」と、カードアプリから端末アプリに送られる「レスポンス」とが基本になると規定されている。従って、国際標準規格を満たすＩＣカードは、受動的な動作しかできず、（２－１）のインストール要求を自ら携帯電話１０に送信することができない。

そのため、携帯電話１０は、国際標準規格を満たすコンビカード２０の場合には、ユーザが携帯電話１０をゲート４０に翳した時点から、非接触通信の状態を監視するためにコンビカード２０にポーリング信号を送り続ける。そして、コンビカード２０から非接触通信終了の応答を受けると、コンビカード２０に対し、要求が有れば送信するように指示し、コンビカード２０は、これに応えてインストール要求を携帯電話１０に送信する（２－１）。

こうした手順を採ることにより、国際標準規格を満たすＩＣカードにも対応することができる。

【００２４】

なお、ここでは、ＩＣカードがコンビカードである場合について説明したが、ＩＣカードが接触通信機能のみを有するときは、図４に示すように、携帯電話１０の赤外線（またはＢｌｕｅｔｏｏｔｈや無線ＬＡＮ）等のローカル通信手段１３を利用して、ＩＣカード２０とゲート４０との通信を行うことができる。この場合、ゲート４０が、通信手段４４

と携帯電話１０のローカル通信手段１３との通信（赤外線）接続を確立して、携帯電話１０にＩＣカード２０へのアクセス命令を送ると、携帯電話１０はＩＣカード２０との接触通信接続を実行し、ゲート４０とＩＣカード２０との通信が可能になる。ゲート４０、ＩＣカード２０及び携帯電話１０の三者間におけるデータのシーケンスは、図３と同じである。

【００２５】

また、ＩＣカードが非接触通信機能のみを有するときには、携帯電話１０およびゲート４０と非接触通信を用いて通信を行う。ユーザが携帯電話１０をゲート４０に翳した時点から、ゲート４０との処理状態を監視するために非接触ＩＣカード２０に問合せを行う。そして、非接触ＩＣカード２０は、ゲート４０との処理が終了すると、携帯電話１０に終了通知を返し、この結果携帯電話１０は非接触ＩＣカード２０に対し、要求が有れば送信するように指示し、非接触ＩＣカード２０は、これに応えてインストール要求を携帯電話１０に送信する（２－１）。または、非接触ＩＣカード２０は、ゲート４０との処理が終了すると、携帯電話１０に終了通知とともにインストール要求を携帯電話１０に送信する（２－１）。

【００２６】

（第２の実施形態）

本発明の第２の実施形態では、ＩＣカードとゲートとの認証成功を条件に、ＩＣカードに格納されたカードアプリの利用が、端末に対して許可される場合について説明する。

ゲートは、ＩＣカードとの認証に成功すると、ＩＣカードに、端末での利用を許容するカードアプリのＩＤと、ゲートを特定するゲートＰＩＮ情報とを伝え、このカードアプリＩＤとゲートＰＩＮとの対情報がＩＣカードに格納される。ＩＣカードは、端末からカードアプリを指定して、その利用が要求されたとき、この対情報を参照して、カードアプリの利用を許可するか否かを決定する。

【００２７】

図５は、この処理を連携して行う携帯電話１０、コンビカード２０及びゲート４０の構成について示している。コンビカード２０は、第１の実施形態（図１）と同様に、非接触通信手段（３）２２、接触通信手段（２）２１、認証情報ＤＢ２５、認証アプリ２４及びＣＰＵ２３を備え、さらに、ゲート４０との認証に成功した場合に有効になるカードアプリ２８と、カードアプリＩＤとゲートＰＩＮとの対情報を格納するＰＩＮＤＢ２９とを備えている。また、携帯電話１０は、接触通信手段（１）１１、ＣＰＵ１２の他に、カードアプリ２８を利用する端末アプリ１４を備えている。ゲート４０の構成は第１の実施形態（図１）と変わりが無い。

【００２８】

このコンビカード２０の認証情報ＤＢ２５には、図６に示すように、ゲートアプリ４３のＩＤと対応付けて、認証処理に使用する認証情報と、ゲートＰＩＮの設定が可能な（即ち、ゲート４０から入場したエリアで利用可能な）カードアプリのＩＤと、ＰＩＮ設定を解除する（即ち、そのエリアで利用できなくなる）カードアプリのＩＤとが格納されている。

ゲート４０から入場したエリアで利用可能になるカードアプリ２８は、例えば、所内の内線番号電話帳アプリであり、コンビカード２０とゲート４０との認証が成功すると、携帯電話１０の電話帳機能を実行する端末アプリ１４からコンビカード２０に格納された内線簿にアクセスできるようになる。

【００２９】

図７は、このゲート４０、コンビカード２０及び携帯電話１０が連携して行う処理のシーケンスを示している。

ユーザがコンビカード２０を装着した携帯電話１０をゲート４０に翳すと、ゲート４０は、コンビカード２０に認証アプリＩＤとゲートアプリＩＤとを示して相互間の認証処理を要求する（１－１）。これを受けてコンビカード２０の認証アプリ２４は、認証情報ＤＢ２５のゲートアプリＩＤに対応する認証情報を用いて、ゲートアプリ４３との認証処理

を実行する（１－２）。認証処理に成功したゲートアプリ４３は、ゲートＰＩＮを設定したい（または削除したい）カードアプリのＩＤとゲートＰＩＮとを提示して、カードアプリＩＤとゲートＰＩＮとの対情報の登録（または削除）を認証アプリ２４に要求する（１－３）。このときゲートアプリ４３が提示するカードアプリＩＤの数は、複数であっても良い。

【００３０】

コンビカード２０の認証アプリ２４は、そのカードアプリＩＤに該当するカードアプリ２８にゲートアプリＩＤとゲートＰＩＮとの情報を送り、確認（検証）を要求する（２－１）。カードアプリ２８は、認証情報ＤＢ２５を参照して、ゲートアプリとの対応関係を有しているか否か（ゲートＰＩＮの設定が可能であるか否か）を検証し、検証結果を認証アプリ２４に返す（２－２）。認証アプリ２４は、検証結果がＯＫである場合に、検証されたカードアプリＩＤとゲートＰＩＮとの対情報をＰＩＮＤＢ２９に格納し（２－３）、検証結果をゲートアプリ４３に通知する（２－４）。

以上がゲート通過時に行われる処理である。

【００３１】

一方、携帯電話１０の端末アプリ１４がカードアプリ２４を利用する場合には、次の処理が行われる。

携帯電話１０の端末アプリ１４は、カードアプリＩＤを提示して、コンビカード２０のカードアプリ２８にアクセスを要求する（３－１）。カードアプリ２８は、認証アプリ２４に、カードアプリＩＤを示して検証結果を要求する（３－２）。認証アプリ２４は、ＰＩＮＤＢ２９を参照し、そのカードアプリＩＤとゲートＰＩＮとの対情報が記録されているときはＯＫを応答し、記録されていないときはＮＧを応答する（３－３）。カードアプリ２８は、認証アプリ２４からの応答がＯＫである場合に、端末アプリ１４に対してアクセスを許可する（３－５）。

【００３２】

こうした処理により、ユーザが正しいゲート４０から入場した場合にのみ、カードアプリ２８の利用を可能にすることができ、例えば、ユーザがＩＣカードを装着した携帯電話を正規のゲートに翳してオフィスに入場すると、ＩＣカードに格納されたオフィス用の内線番号電話帳アプリが自動的に有効になる。

【００３３】

なお、ゲートアプリ４３から提示されたカードアプリＩＤがＰＩＮ設定を解除するカードアプリＩＤとして認証情報ＤＢ２５に記録されている場合には、認証アプリ２４は、ＰＩＮＤＢ２９を参照し、そこに記録されているカードアプリＩＤとゲートＰＩＮとの対情報を削除する。

このようにＰＩＮＤＢ２９の削除処理を併せて行うことにより、例えば、ユーザが、入門処理をして、あるオフィスに入場した後、別のオフィスに入門処理をして入場した場合に、先のオフィス用の内線番号電話帳アプリが無効になり、後から入場したオフィス用の内線番号電話帳アプリだけが有効になる。

【００３４】

なお、各処理のメッセージ及びデータは、第三者の盗聴を防ぐために暗号化して送信するようにしても良い。

また、図７において、（２－３）の検証結果の格納は、カードアプリＩＤの検証結果がＯＫであることを示す情報だけをＰＩＮＤＢ２９に格納するようにしても良い。

また、ＩＣカードは、接触通信機能のみを有するものであっても良い。この場合には、第１の実施形態（図４）で説明したように、携帯電話１０のローカル通信手段を利用してＩＣカードとゲートとの通信を行う。

また、ＩＣカードは、非接触通信機能のみを有するものであっても良い。

【００３５】

なお、図６に示す認証情報ＤＢにおいて、一つのゲートアプリＩＤに対し、複数のカードアプリＩＤが設定されている場合には、端末アプリのアクセスを許容するカードアプリ

に優先度を設定することも可能である。この場合、図８に示すように、ゲートアプリＩＤに対応して、優先度設定可能なカードアプリＩＤ及び優先度設定を解除できるカードアプリＩＤの優先度を設定した優先設定ＤＢを保持する。あるいは、図９に示すように、各カードアプリＩＤの優先度を優先度テンプレート（ｂ）で規定し、ゲートアプリＩＤに対応して優先度テンプレートを設定した優先設定ＤＢ（ａ）を保持する。

そして、認証情報ＤＢから、ゲートアプリＩＤに対応するカードアプリを選択する場合に、優先設定ＤＢを参照し、優先度に基づいて選択するカードアプリを決定する。

【００３６】

（第３の実施形態）

本発明の第３の実施形態では、ＩＣカードとゲートとの認証成功を条件に、ＩＣカードに格納されたカードアプリの利用が、端末に対して許可される第２の実施形態の構成において、ＩＣカード、ゲート及び端末の三者間での処理が、第２の実施形態と異なる手順で行われる場合について説明する。

【００３７】

ここでは、図１０に示すように、機器１が、非接触通信手段（１）１１０を有するドア１００であり、機器２が、非接触通信手段２２のみを有するＩＣカード２００であるものとして説明する。機器１、機器２及び機器３のその他の構成は、第２の実施形態（図５）と変わりがない。

ここでは、非接触通信手段２２のみを有するが、接触通信手段のみを有しても良い。

【００３８】

図１１は、ゲート４０、ＩＣカード２００及びドア１００が連携して行う処理のシーケンスを示している。

ユーザがＩＣカード２００をゲート４０に翳すと、ゲート４０は、ＩＣカード２００に認証アプリＩＤとゲートアプリＩＤとを示して相互間の認証処理を要求する（１－１）。これを受けてＩＣカード２００の認証アプリ２４は、認証情報ＤＢ２５のゲートアプリＩＤに対応する認証情報を用いて、ゲートアプリ４３との認証処理を実行する（１－２）。認証処理に成功したゲートアプリ４３は、ゲートＰＩＮを設定するカードアプリのＩＤとゲートＰＩＮとを提示して、カードアプリＩＤとゲートＰＩＮとの対情報の登録を認証アプリ２４に要求し（１－３）、ＩＣカード２００の認証アプリ２４は、要求に従ってカードアプリＩＤとゲートＰＩＮとの対情報をＰＩＮＤＢ２９に登録する（１－４）。この登録の段階では、認証情報ＤＢ２５との検証は済んでいない。

以上がゲート通過時に行われる処理である。

【００３９】

一方、ユーザがＩＣカード２００をドア１００に翳すと、次の処理が行われる。

ドア１００の端末アプリ１４は、端末アプリＩＤとカードアプリＩＤとを提示して、ＩＣカード２００のカードアプリ２８へのアクセスを要求する（２－１）。カードアプリ２８は、認証アプリ２４に、カードアプリＩＤとゲートアプリＩＤとを示してＰＩＮＤＢ２９の登録情報を要求し（２－２）、認証アプリ２４は、ＰＩＮＤＢ２９から、該当するカードアプリＩＤ及びゲートＰＩＮの対情報を取得してカードアプリ２８に提示する（２－３）。カードアプリ２８は、認証情報ＤＢ２５を参照して、ゲートアプリとの対応関係を有しているか（ゲートＰＩＮの設定が可能であるか）を検証し（２－４）、検証結果がＯＫである場合に、端末アプリ１４にアクセスを許可する（２－５）。

カードアプリ２８にアクセスしたドア１００の端末アプリ１４は、例えば、カードアプリ２８から鍵情報を取得してドア１００を開錠し、ユーザは、ドア１００の通過が可能になる。

【００４０】

このように、ゲート４０、ＩＣカード２００及びドア１００が連携することにより、正しい玄関（ゲート）から入らないと、ドアが開かないようにすることができる。

また、このＰＩＮ検証（２－４）では、カードアプリ２８が、端末アプリ１４とゲートＰＩＮとのペアを検証することも可能であり、この場合には、ある端末アプリ１４につい

て、特定のゲートＰＩＮと対応していなければアクセスを許可しない（即ち、あるドアは特定の入口から入らないと開かない）と言う制御を行うこともできる。

【００４１】

また、図１２に示すように、ドア１００にＰＩＮ入力部１５を設け、ユーザがＰＩＮ入力部１５から入力したユーザＰＩＮをさらに検証して、ドア１００を開けるように制御することもできる。

図１３は、この場合のシーケンスを示している。ゲートＰＩＮを検証する（２－４）までの処理は、図１１の場合と同じである。ゲートＰＩＮの検証結果がＯＫである場合に、カードアプリ２８は、ドア１００にユーザＰＩＮを要求し（２－５）、ユーザがＰＩＮ入力部１５からユーザＰＩＮを入力すると（２－６）、カードアプリ２８は、ＩＣカード２００のＰＩＮＤＢ２９で保持されたユーザＰＩＮと照合して、それを検証する（２－７）。そして、検証結果が一致する場合に、端末アプリ１４に対してアクセスを許可する（２－８）。

【００４２】

（第４の実施形態）

本発明の第４の実施形態では、ＩＣカードとゲートとの認証処理が成功したことを条件に、機器の処理が可能になる場合について説明する。

ＩＣカードは、ゲートとの認証処理が成功すると、ゲートからゲートＰＩＮを取得し、このゲートＰＩＮを機器に送信する。機器は、ゲートＰＩＮの検証が終了した後、処理を開始する。

【００４３】

図１４は、ゲート４０、コンビカード２０及び携帯電話１０の構成と、機器（機器４）が金庫５０である場合の構成とを示している。このコンビカード２０を装着した携帯電話１０をゲート４０に翳し、コンビカード２０とゲート４０との認証処理を行う。認証が成功した場合に、この携帯電話１０を金庫５０に翳し、また、携帯電話１０からユーザＰＩＮを入力することにより、金庫５０の開錠が可能になる。

金庫５０は、コンビカード２０への非接触通信を行う非接触通信手段（５）５１と、金庫５０の鍵の開閉を制御する鍵アプリ５３と、金庫５０の動作を制御するＣＰＵ５２とを備えている。ゲート４０、コンビカード２０及び携帯電話１０の構成は、第２の実施形態（図１０）と変わりがない。

【００４４】

コンビカード２０を装着した携帯電話１０をゲート４０に翳すと、ゲート４０とコンビカード２０との間で、図１３の（１－１）から（１－４）までの処理が行われる。

図１５は、その後、ユーザが、コンビカード２０を装着した携帯電話１０を金庫５０に翳したときの処理シーケンスを示している。

金庫５０の鍵アプリ５３は、カードアプリＩＤを示して、コンビカード２０にカードアプリ２９へのアクセスを要求する（３－１）。カードアプリ２９は、カードアプリＩＤ及び鍵アプリＩＤを提示して、認証アプリ２４にゲートＰＩＮを要求する（３－２）。認証アプリ２４は、ＰＩＮＤＢ２９を参照し、カードアプリＩＤに対応するゲートＰＩＮ情報を取得してカードアプリ２９に返す（３－３）。

【００４５】

次に、カードアプリ２９は、携帯電話１０の端末アプリ１４にユーザＰＩＮを要求する（３－４）。端末アプリ１４は、ＰＩＮ入力画面を表示し、ユーザがＰＩＮを入力すると（３－５）、そのユーザＰＩＮをカードアプリ２９に送信する（３－６）。カードアプリ２９は、コンビカード２０のＰＩＮＤＢ２９で保持されているユーザＰＩＮ情報と照合して、それを検証する（３－７）。ユーザＰＩＮの検証結果が一致した場合は、ゲートＰＩＮを金庫の鍵アプリ５３に送信する（３－８）。鍵アプリ５３は、予め保持するゲートＰＩＮ情報と、カードアプリ２９から送られたゲートＰＩＮとを照合して検証し（３－９）、検証結果が一致する場合に、開錠処理を実行する（３－１０）。

このように、例えば、ゲート４０が玄関に設置されている場合では、玄関での入門処理

が正しく行われたときにのみ、金庫５０の鍵が使えることになる。

【００４６】

なお、ユーザＰＩＮやゲートＰＩＮの検証を行う時期、あるいは、検証を行う主体等については、種々の変更が可能である。例えば、鍵アプリ５３がゲートＰＩＮの検証（３－９）を行う代わりに、カードアプリ２９が、ユーザＰＩＮ検証（３－８）とともに、ゲートＰＩＮの検証を行い、検証結果を鍵アプリ５３に伝えるようにしても良い。

また、カードアプリ２９がユーザＰＩＮ検証（３－８）を行う代わりに、入力されたユーザＰＩＮを鍵アプリ５３に送り、鍵アプリ５３が、金庫５０に登録されたユーザＰＩＮと照合してユーザＰＩＮ検証を行うようにしても良い。

【００４７】

また、図１６に示すように、ＰＩＮ登録（４－４）を終了した認証アプリ２４が、端末アプリ１４にユーザＰＩＮを要求し（４－５）、入力されたユーザＰＩＮをそのままＰＩＮＤＢ２９に登録（４－８）するようにしても良い。この場合は、図１７に示すように、携帯電話１０を金庫５０に翳した段階で、カードアプリ２９が、ＰＩＮＤＢ２９からゲートＰＩＮ及びユーザＰＩＮを取得し（５－３）、ユーザＰＩＮを検証し（５－４）、ゲートＰＩＮを金庫５０の鍵アプリ５３に送る（５－５）。この方式では、ユーザのＰＩＮ入力が事前に済んでいるため、金庫５０の前でのユーザの入力操作が不要になる。

【００４８】

また、図１８に示すように、ＰＩＮ登録（４－４）が終了した時点で、その通知を受けたカードアプリ２８が、ユーザＰＩＮを要求し（４－６）、入力されたユーザＰＩＮを検証して（４－８）、検証結果を登録する（４－１０）ようにしてもよい。この場合は、図１９に示すように、携帯電話１０を金庫５０に翳した段階で、ユーザの検証結果をチェックする（５－４）だけで足りる。この方式では、ユーザＰＩＮ検証が早い段階で行われるため、ユーザがＰＩＮ入力を間違えていた場合に、早い段階で修正できる。

【００４９】

また、図２０は、コンビカード（機器２）のカードアプリ（アプリ２）が、ユーザＰＩＮ要求と、ゲートＰＩＮ検証と、ユーザＰＩＮ検証とを行う場合のシーケンスを示している。

また、図２１は、コンビカード（機器２）のカードアプリ（アプリ２）が、ユーザＰＩＮ要求と、ユーザＰＩＮ検証とを行い、金庫（機器４）の鍵アプリ（アプリ５）がゲートＰＩＮ検証を行う場合のシーケンスを示している。

また、図２２は、コンビカード（機器２）のカードアプリ（アプリ２）が、ユーザＰＩＮ要求と、ゲートＰＩＮ検証とを行い、金庫（機器４）の鍵アプリ（アプリ５）がユーザＰＩＮ検証を行う場合のシーケンスを示している。

【００５０】

また、図２３は、コンビカード（機器２）の認証アプリ（アプリ３）が、ユーザＰＩＮ要求を行い、金庫（機器４）の鍵アプリ（アプリ５）がゲートＰＩＮ検証と、ユーザＰＩＮ検証とを行う場合のシーケンスを示している。

また、図２４は、ユーザＰＩＮ入力を金庫（機器４）から行い、金庫（機器４）の鍵アプリ（アプリ５）がゲートＰＩＮ検証と、ユーザＰＩＮ検証とを行う場合のシーケンスを示している。

また、図２５は、ユーザＰＩＮ入力を金庫（機器４）から行い、コンビカード（機器２）のカードアプリ（アプリ２）が、ユーザＰＩＮ検証を行い、金庫（機器４）の鍵アプリ（アプリ５）がゲートＰＩＮ検証を行う場合のシーケンスを示している。

また、図２６は、ユーザＰＩＮ入力を金庫（機器４）から行い、コンビカード（機器２）のカードアプリ（アプリ２）が、ゲートＰＩＮ検証を行い、金庫（機器４）の鍵アプリ（アプリ５）がユーザＰＩＮ検証とを行う場合のシーケンスを示している。

【００５１】

コンビカード（機器２）のカードアプリ（アプリ２）でゲートＰＩＮを検証する場合は、ゲートＰＩＮが変わった場合に、カード内に格納されたゲートＰＩＮを変更すれば足り

る。また、ゲートアプリ（アプリ４）と鍵アプリ（アプリ５）の組み合わせでアクセス制御を行うことができる。

また、金庫（機器４）の鍵アプリ（アプリ５）でゲートＰＩＮを検証する場合は、新しい金庫（機器４）が追加された時に、その金庫にゲートＰＩＮ情報を登録するだけで足りる。また、金庫を削除するときに、カードの設定を変える必要がない。

【００５２】

また、コンビカード（機器２）のカードアプリ（アプリ２）でユーザＰＩＮを検証する場合は、ユーザがユーザＰＩＮを変えたい場合に、コンビカード（機器２）に格納されているユーザＰＩＮを変更するだけで足り、わざわざユーザＰＩＮを換えたい機器（例えば金庫）のところに赴いて変えなくても済む。また、一つのユーザＰＩＮが複数の機器（ドアなど）に対応している場合でも、ドアごとにユーザＰＩＮを設定して回らなくて済む。また、図１８に示すように、ユーザＰＩＮを事前入力する場合に、ユーザＰＩＮの入力時に金庫（機器４）無しで検証が行えるので、金庫に翳してからユーザＰＩＮの再入力が必要になるような事態は発生しない。

また、金庫（機器４）の鍵アプリ（アプリ５）でユーザＰＩＮを検証する場合は、金庫でユーザＰＩＮを管理しているので、何人のユーザが登録されているのかが容易に把握できる。

【００５３】

また、本実施の形態では、機器４を金庫、カードアプリとして鍵アプリを想定したが、機器４をビデオやセットトップボックス（ＳＴＢ）、カードアプリとして、決済カードアプリや、有料放送録画予約アプリ、有料放送受信操作アプリを想定してもよい。こうすることにより、正しく玄関の鍵の処理をしていないと、ＳＴＢ（ＰＣ）を介した決済処理（決済カードアプリ）ができない、ビデオ録画予約（その解除）（有料放送録画アプリ）ができない、といったサービスも可能である。

また、機器４を車の防犯モジュールとした場合、正しく玄関の鍵を閉じる処理をしたカードアプリと防犯モジュール（機器４）で正しいチェックイン処理をしないまま、車のドアを開けたり、車のエンジンをかけたり、車のオーディオを外したりすると防犯ベルが鳴るといったサービスも可能である。

【００５４】

なお、実施形態では、主に、ＩＣカードを携帯電話に装着する場合について説明したが、本発明はこれに限定されるものではない。携帯電話に代えて、ＰＤＡ（Personal Digital Assistant）、メール端末、小型パーソナルコンピュータ、ゲーム機など、各種の端末装置・情報処理装置を用いることができる。また、ＩＣカードは、国際標準規格を満たすものでも、満たさないものでも使用可能である。セキュアデバイスの形状は、カード状でもチップ状でも良く、情報処理装置に埋め込む形態であっても良い。

また、ＩＣカードは接触通信手段のみを有しても良い。

【産業上の利用可能性】

【００５５】

本発明は、各種のセキュアデバイスの機能や、各種の端末、装置、機器等の機能を場所、経路、位置等との関連で変える場合に利用することができ、オフィス、家庭、医療現場、教育現場など、あらゆる分野での利用が可能である。

【図面の簡単な説明】

【００５６】

【図１】本発明の第１の実施形態における携帯電話、コンビカード及びゲートの構成を示すブロック図

【図２】本発明の第１の実施形態における認証情報ＤＢのデータ構成を示す図

【図３】本発明の第１の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス

【図４】本発明の第１の実施形態における携帯電話、ＩＣカード及びゲートの構成を示すブロック図

【図５】本発明の第２の実施形態における携帯電話、コンビカード及びゲートの構成を示すブロック図
【図６】本発明の第２の実施形態における認証情報ＤＢのデータ構成を示す図
【図７】本発明の第２の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス
【図８】本発明の第２の実施形態における優先度設定ＤＢのデータ構成を示す図
【図９】本発明の第２の実施形態における優先度設定ＤＢの他のデータ構成を示す図
【図１０】本発明の第３の実施形態におけるドア、ＩＣカード及びゲートの構成を示すブロック図
【図１１】本発明の第３の実施形態におけるドア、ＩＣカード及びゲートの動作を示すシーケンス
【図１２】本発明の第３の実施形態におけるＰＩＮ入力部を持つドア、ＩＣカード及びゲートの構成を示すブロック図
【図１３】本発明の第３の実施形態におけるＰＩＮ入力部を持つドア、ＩＣカード及びゲートの動作を示すシーケンス
【図１４】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の構成を示すブロック図
【図１５】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス
【図１６】本発明の第４の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス
【図１７】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス（図１６の続き）
【図１８】本発明の第４の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス
【図１９】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス（図１８の続き）
【図２０】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス
【図２１】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス
【図２２】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス
【図２３】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス
【図２４】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス
【図２５】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス
【図２６】本発明の第４の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

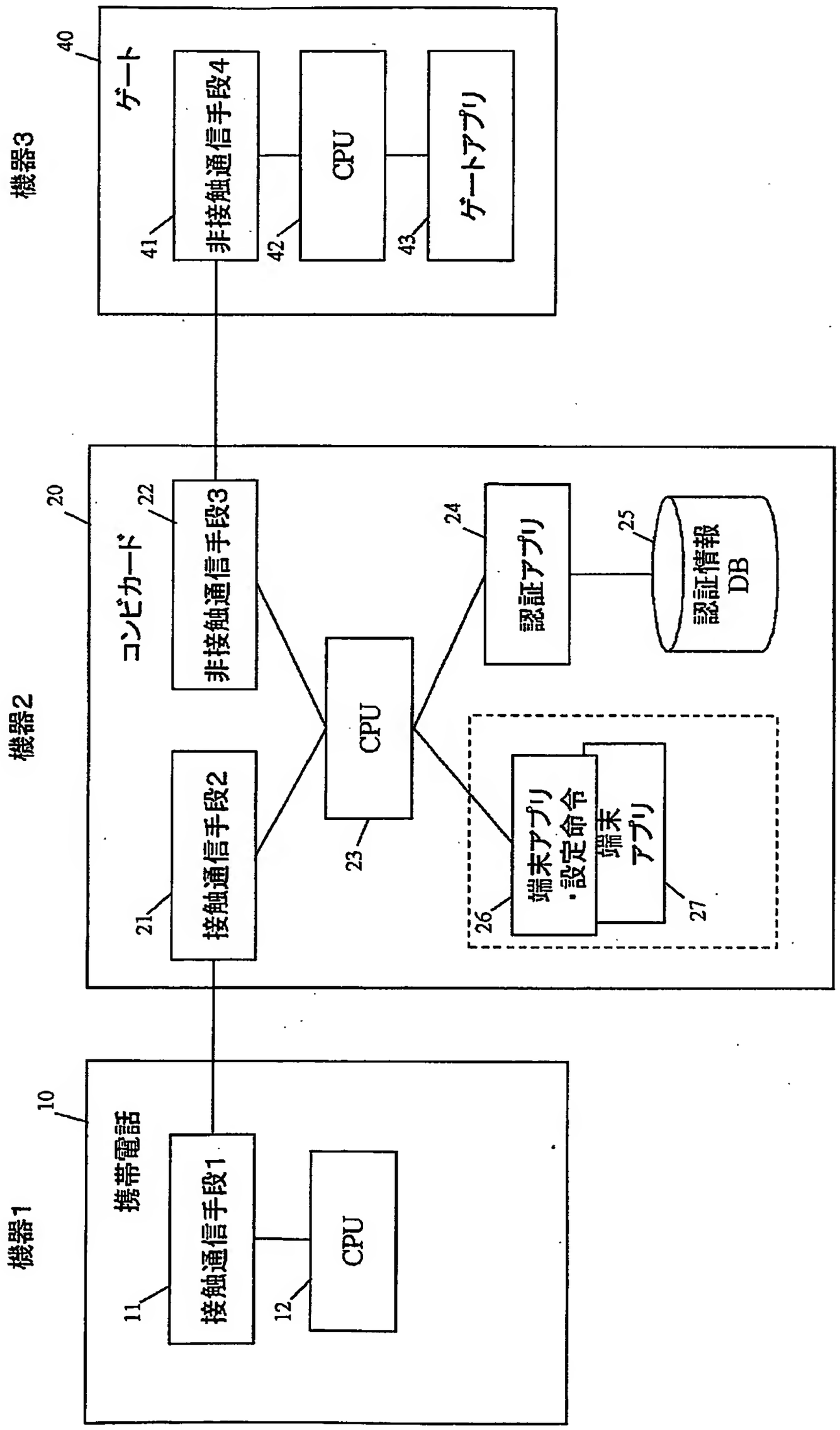
【符号の説明】

【００５７】

１０　携帯電話
１１　接触通信手段（
１２　ＣＰＵ
１３　ローカル通信手段
１４　端末アプリ
１５　ＰＩＮ入力部
２０　コンビカード

２１　接触通信手段
２２　非接触通信手段
２３　ＣＰＵ
２４　認証アプリ
２５　認証情報ＤＢ
２６　端末アプリ・設定命令セット
２７　端末アプリ
２８　カードアプリ
２９　ＰＩＮＤＢ
４０　ゲート
４１　非接触通信手段
４２　ＣＰＵ
４３　ゲートアプリ
４４　通信手段
５０　金庫
５１　非接触通信手段
５２　ＣＰＵ
５３　鍵アプリ
１００　ドア
２００　ＩＣカード

【書類名】図面
【図１】

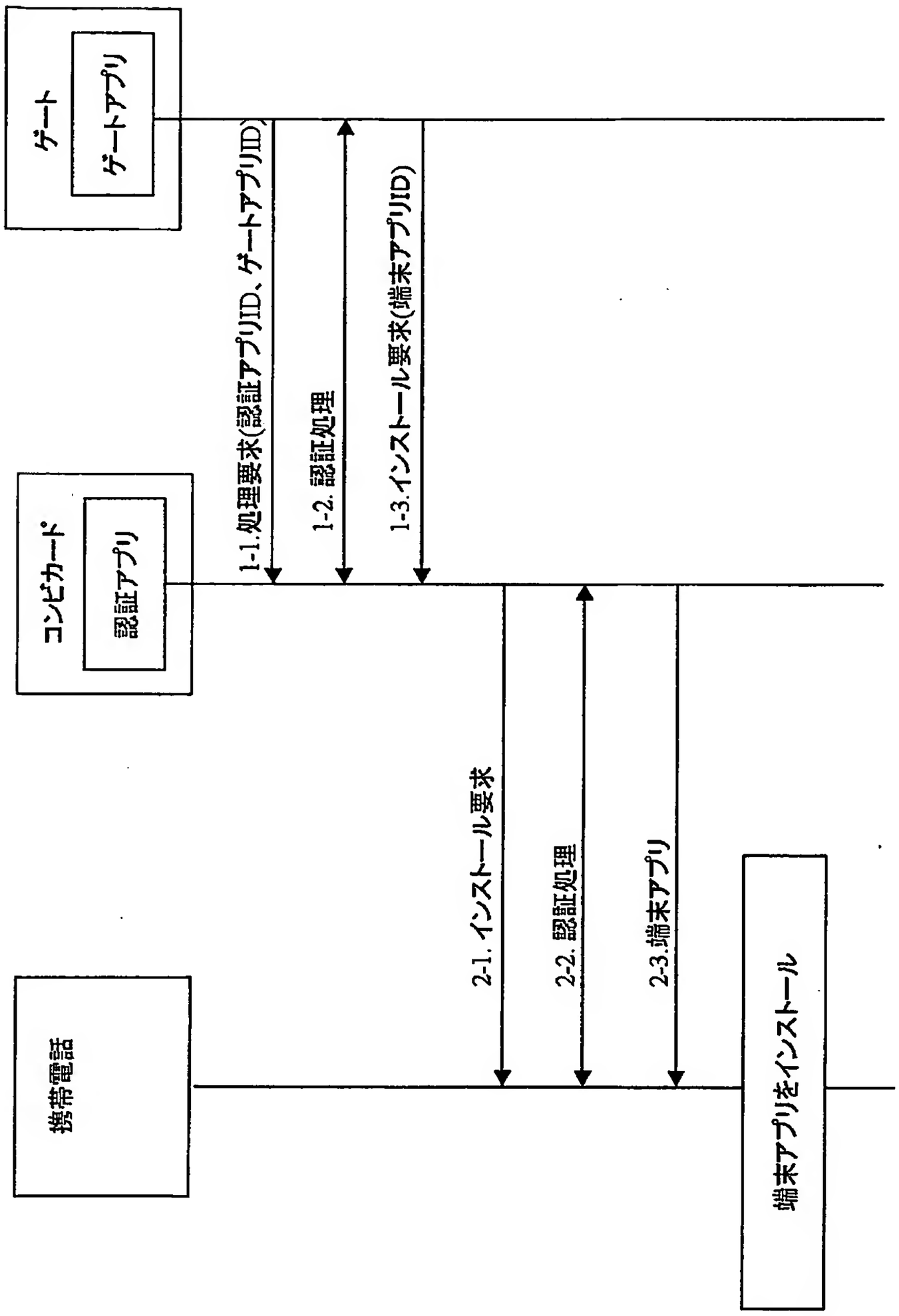

機器3
40
ゲート
非接触通信手段4
41
CPU
42
ゲートアプリ
43
機器2
20
コンビカード
非接触通信手段3
22
接触通信手段2
21
CPU
23
認証アプリ
24
認証情報DB
25
端末アプリ・設定命令
端末アプリ
26
27
機器1
10
携帯電話
接触通信手段1
11
CPU
12

【図２】

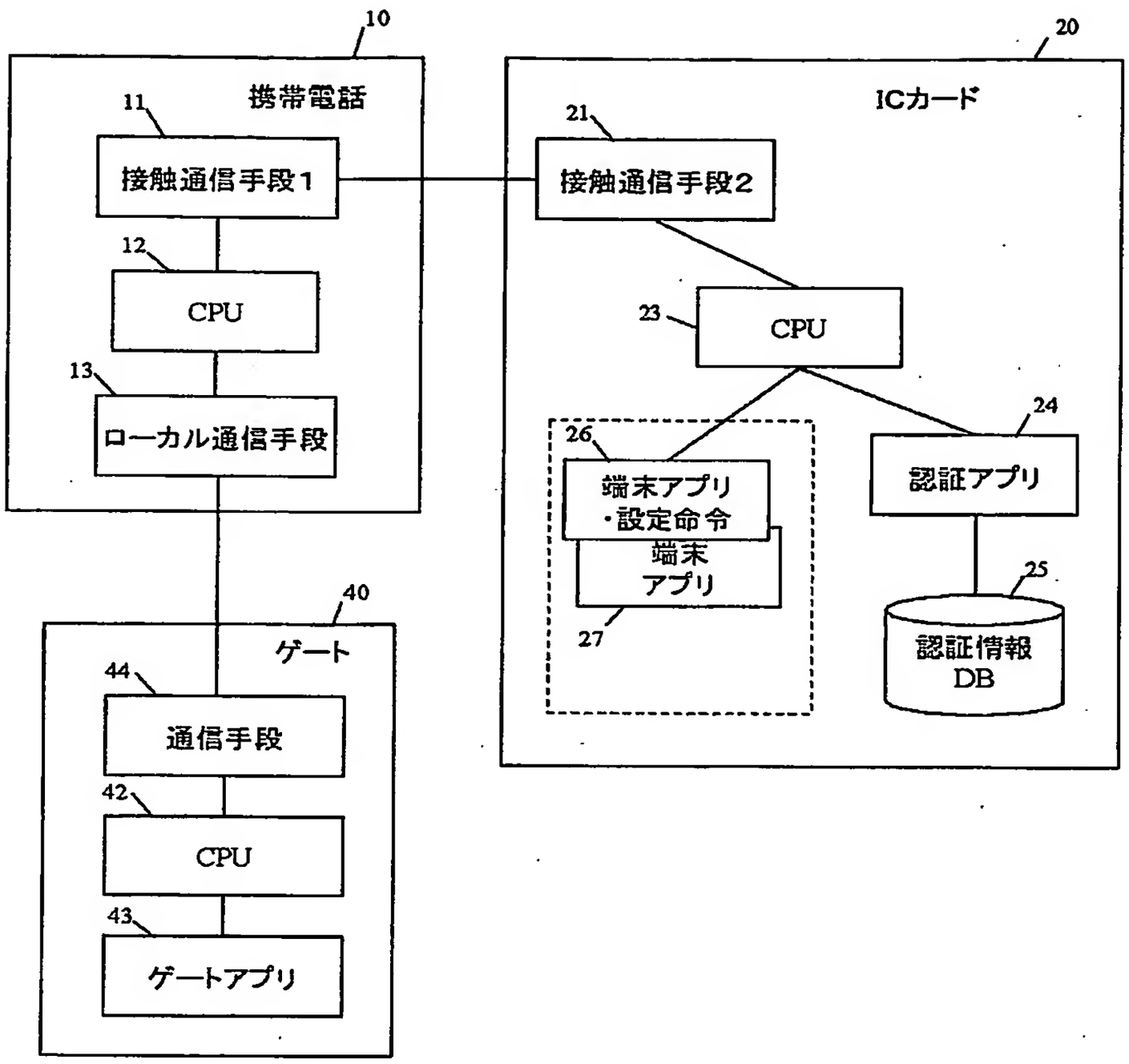
認証情報DB

ゲートアプリID	認証情報	インストール可能な端末アプリＩＤ、設定命令ＩＤ
www.app.co.jp/gate1		端末アプリ１ＩＤ 端末アプリ２ＩＤ 設定命令５ＩＤ

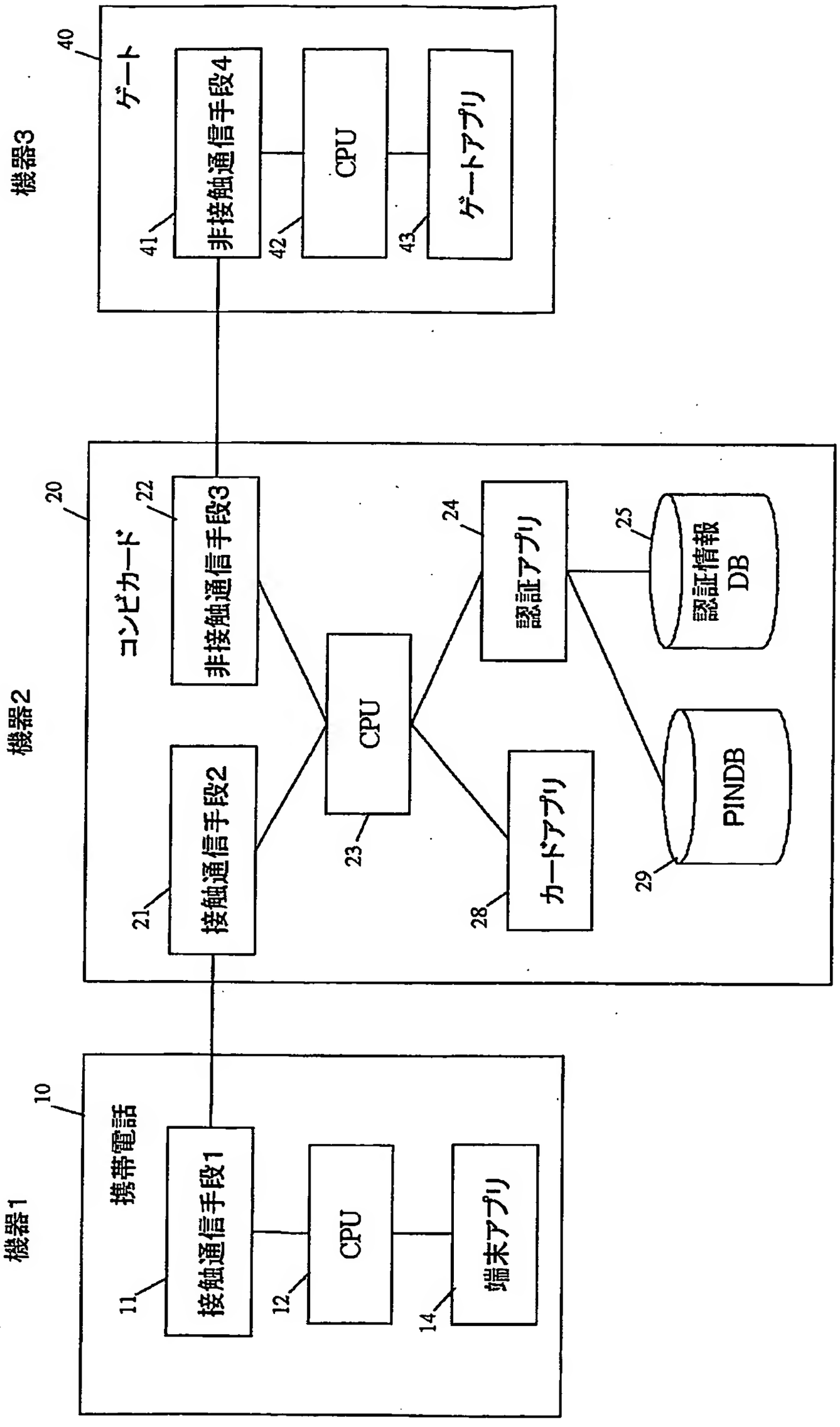
【図３】


ゲート
ゲートアプリ
コンビカード
認証アプリ
携帯電話
1-1.処理要求(認証アプリID、ゲートアプリID)
1-2. 認証処理
1-3.インストール要求(端末アプリID)
2-1. インストール要求
2-2. 認証処理
2-3.端末アプリ
端末アプリをインストール

【図４】


10
携帯電話
11
接触通信手段１
12
CPU
13
ローカル通信手段
20
ICカード
21
接触通信手段2
23
CPU
24
認証アプリ
26
端末アプリ
・設定命令
端末
アプリ
27
25
認証情報
DB
40
ゲート
44
通信手段
42
CPU
43
ゲートアプリ

【図５】

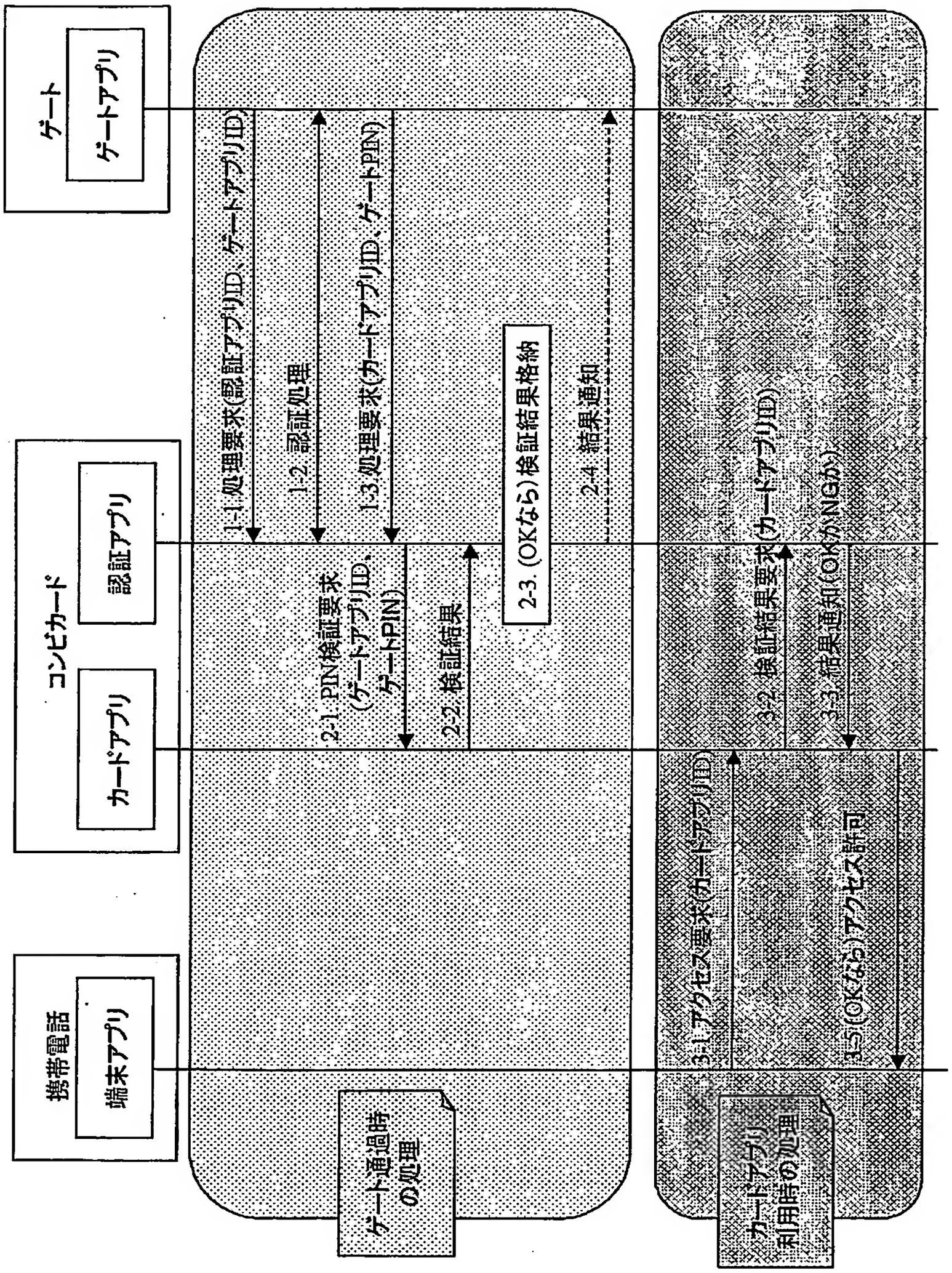

機器3
40
ゲート
非接触通信手段4
41
CPU
42
ゲートアプリ
43
機器2
20
コンビカード
非接触通信手段3
22
接触通信手段2
21
CPU
23
認証アプリ
24
認証情報DB
25
カードアプリ
28
PINDB
29
機器1
10
携帯電話
接触通信手段1
11
CPU
12
端末アプリ
14

【図６】

認証情報DB

アプリID	認証情報	PIN設定可能なカードアプリID	PIN設定を解除するカードアプリID
www.app.co.jp/gate1		カードアプリ１ＩＤ カードアプリ２ＩＤ	カードアプリ３ＩＤ カードアプリ４ＩＤ

【図７】


ゲート
ゲートアプリ
コンビカード
認証アプリ
カードアプリ
携帯電話
端末アプリ
1-1.処理要求(認証アプリID)
1-2.認証処理
1-3.処理要求(カードアプリ
2-1.PIN検証要求
(ゲートアプリID、
ゲートPIN)
2-2.検証結果
2-3.(OKなら)検証結果格納
2-4.結果通知
3-1.アクセス要求(カードアプリID)
3-2.検証結果要求(カードアプリID)
3-3.結果通知(OKかNGか)
3-5.(OKなら)アクセス許可
ゲート通過時
の処理
カードアプリ
利用時の処理

【図８】

アプリID	優先度設定可能なカードアプリID		
www.app.co.jp/gate1	カードアプリ1ID カードアプリ2ID		

優先度設定を解除できるカードアプリID			
カードアプリ3ID カードアプリ4ID			

【図９】

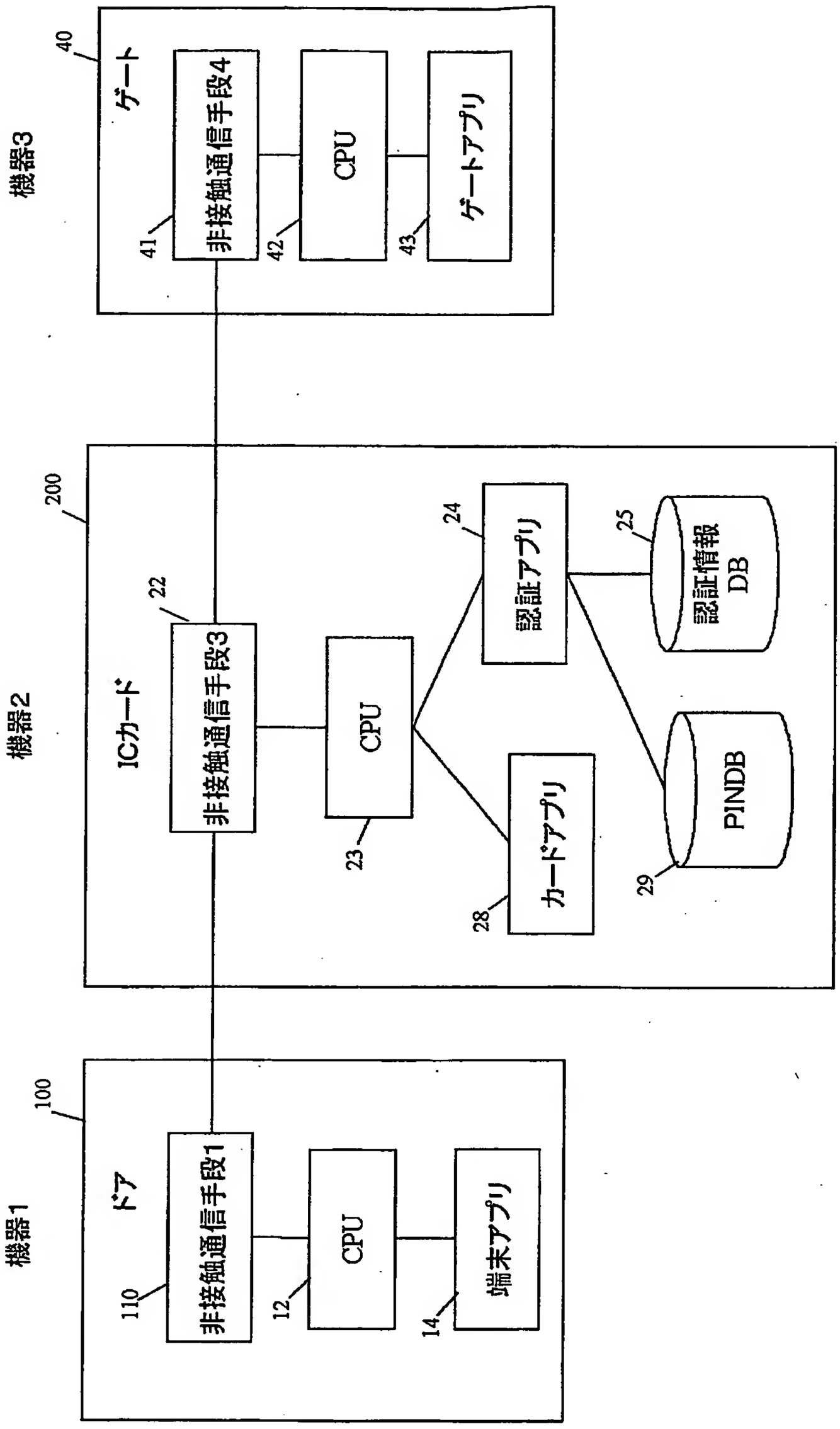
(a)

アプリID	設定可能な優先度テンプレート	解除可能な優先度テンプレート
www.app.co.jp/gate1	テンプレート1のID テンプレート2のID	テンプレート3のID

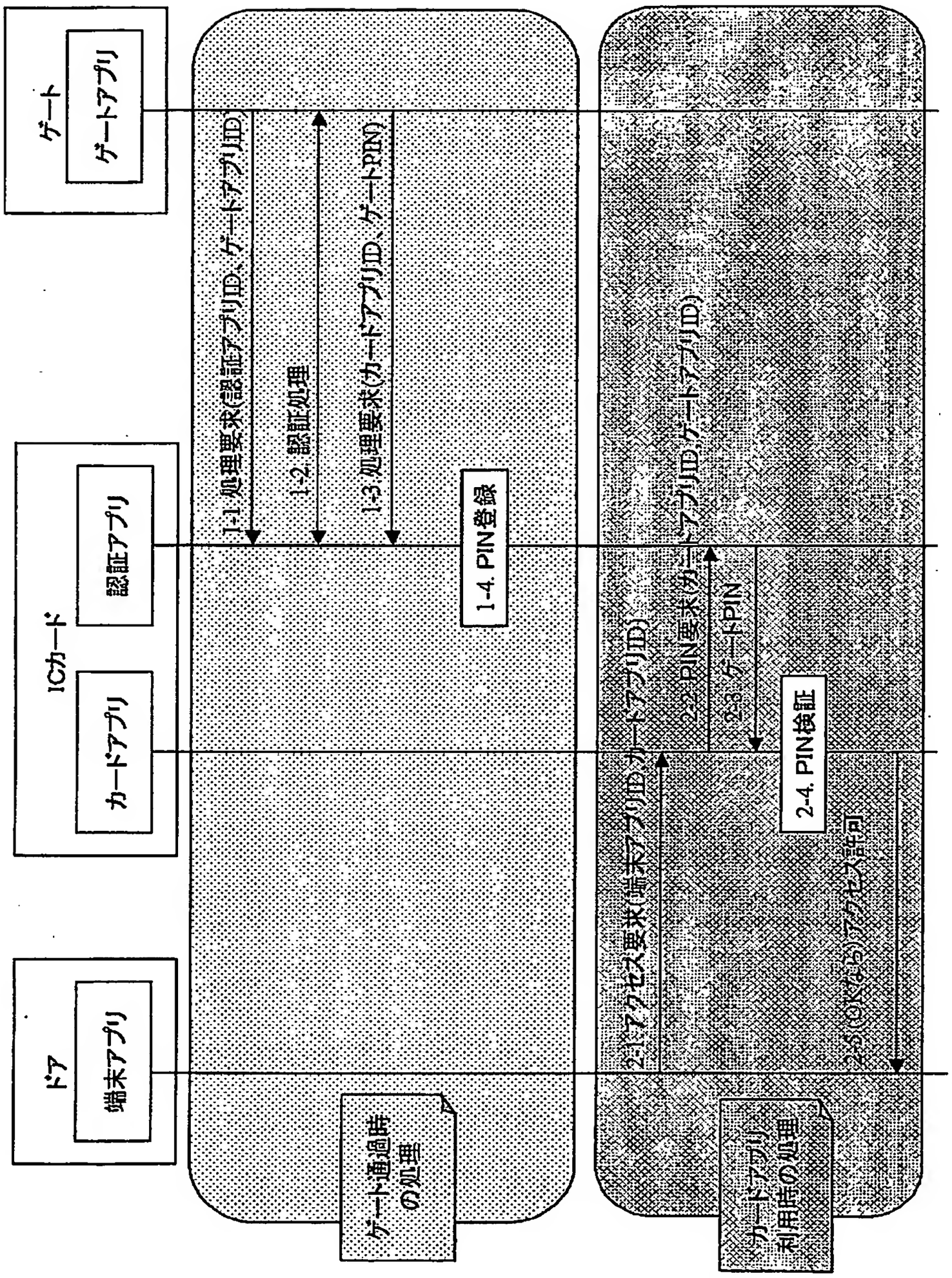
(b)

優先度テンプレートID	5
優先度1	カードアプリ1のID
優先度2	カードアプリ3のID

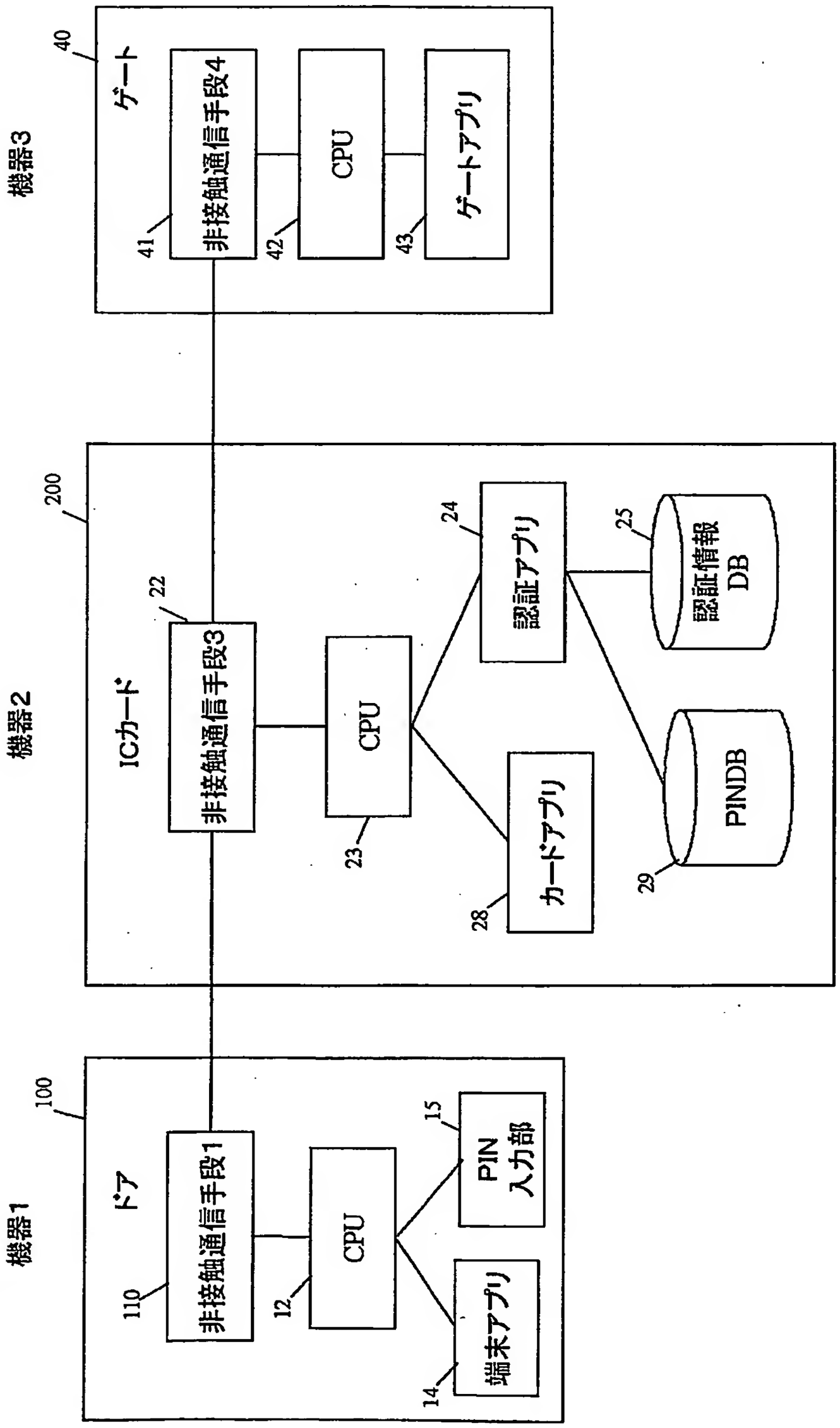
【図１０】


機器3
40
ゲート
非接触通信手段4
41
CPU
42
ゲートアプリ
43
機器2
200
ICカード
非接触通信手段3
22
CPU
23
認証アプリ
24
認証情報DB
25
PINDB
29
カードアプリ
28
機器1
100
ドア
非接触通信手段1
110
CPU
12
端末アプリ
14

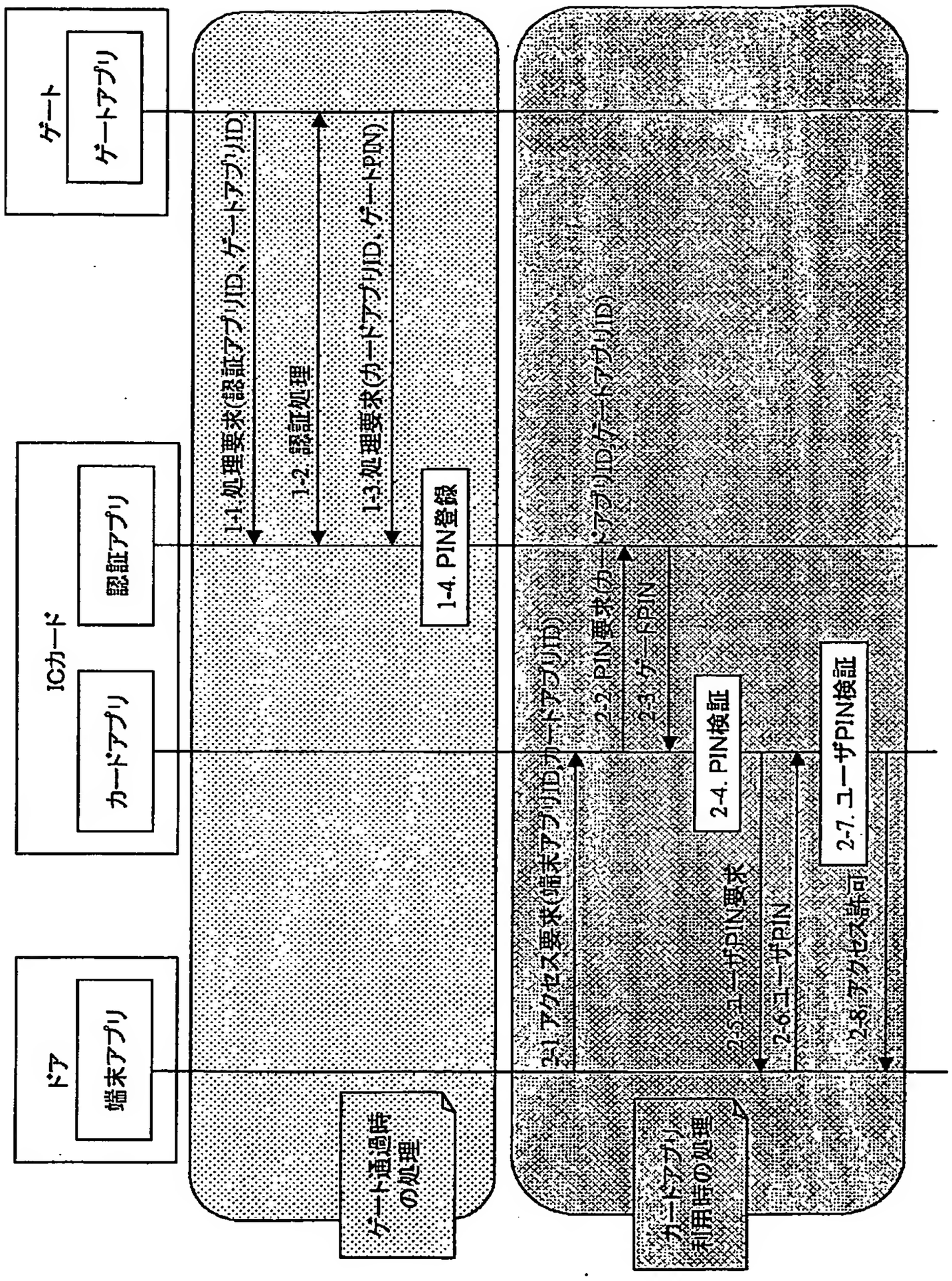
【図１１】


ゲート
ゲートアプリ
ICカード
認証アプリ
カードアプリ
端末アプリ
ドア
1-1. 処理要求(認証アプリID、ゲートアプリID)
1-2. 認証処理
1-3. 処理要求(カードアプリID、ゲートPIN)
1-4. PIN登録
2-1. アクセス要求(端末アプリID,カードアプリID)
2-2. PIN要求(カードアプリID,ゲートアプリID)
2-3. ゲートPIN
2-4. PIN検証
2-5. (OK)カードアプリアクセス許可
ゲート通過時の処理
カードアプリ利用時の処理

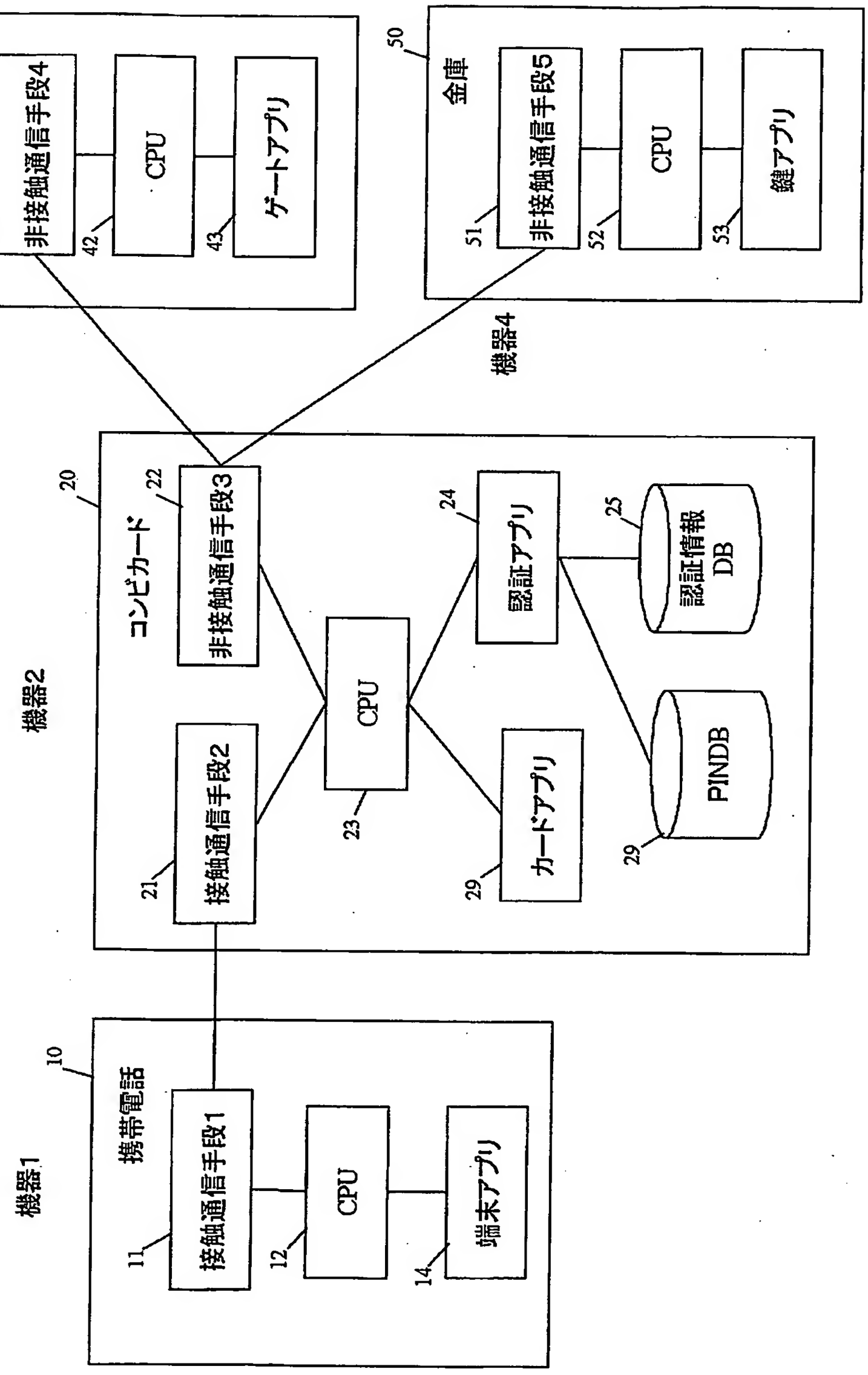
【図１２】


機器3
40
ゲート
非接触通信手段4
41
CPU
42
ゲートアプリ
43
機器2
200
ICカード
非接触通信手段3
22
CPU
23
認証アプリ
24
認証情報DB
25
PINDB
29
カードアプリ
28
機器1
100
ドア
非接触通信手段1
110
CPU
12
PIN入力部
15
端末アプリ
14

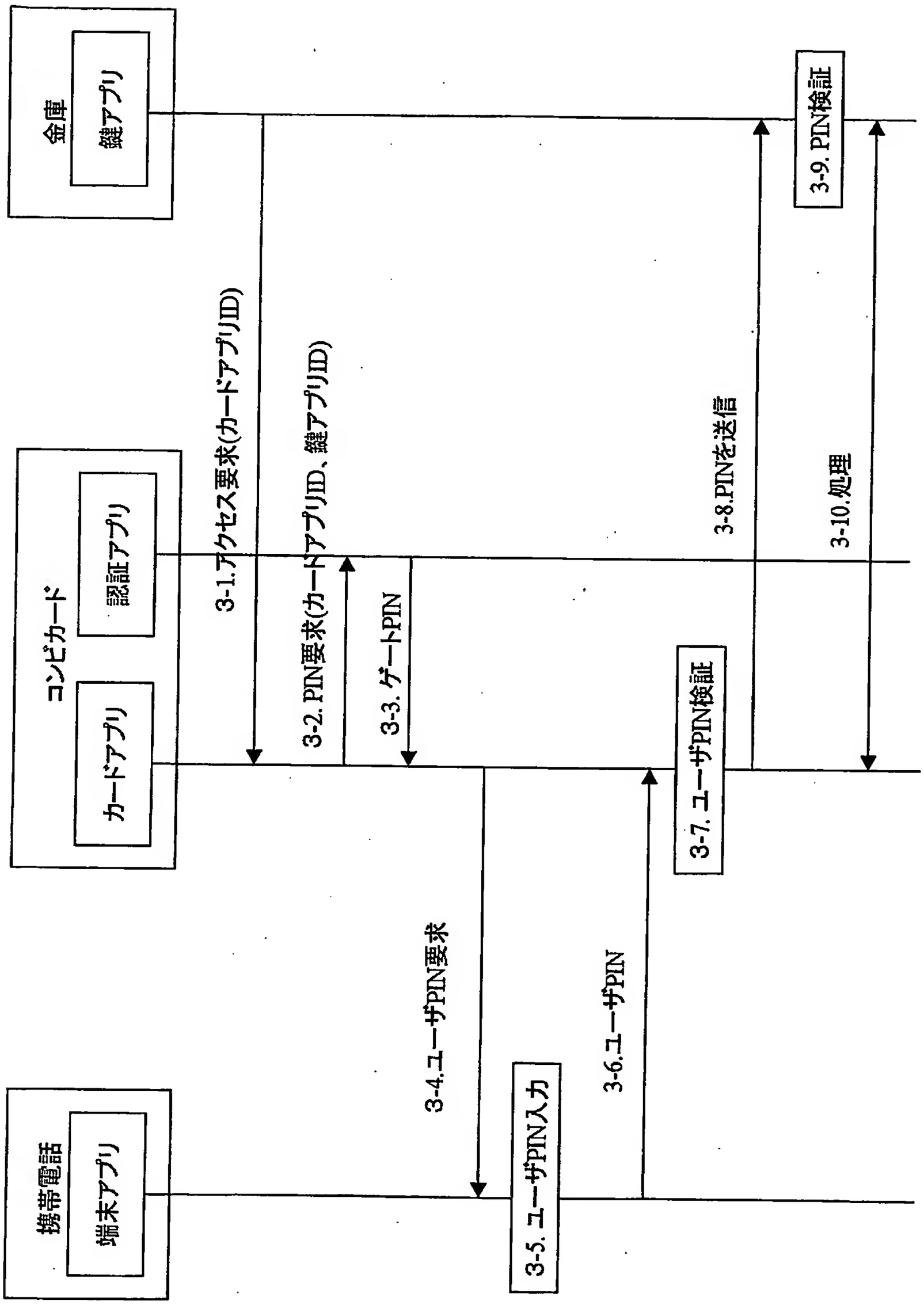
【図１３】


ゲート
ゲートアプリ
ICカード
認証アプリ
カードアプリ
ドア
端末アプリ
1-1.処理要求(認証アプリID、ゲートアプリID)
1-2. 認証処理
1-3.処理要求(カードアプリID、ゲートアプリID、ゲートPIN)
1-4. PIN登録
2-1.アクセス要求(端末アプリID,カードアプリID)
2-2.PIN要求(カードアプリID,ゲートアプリID)
2-3.ゲートPIN
2-4. PIN検証
2-5.ユーザPIN要求
2-6.ユーザPIN
2-7.ユーザPIN検証
2-8.アクセス許可
ゲート通過時の処理
カードアプリ利用時の処理

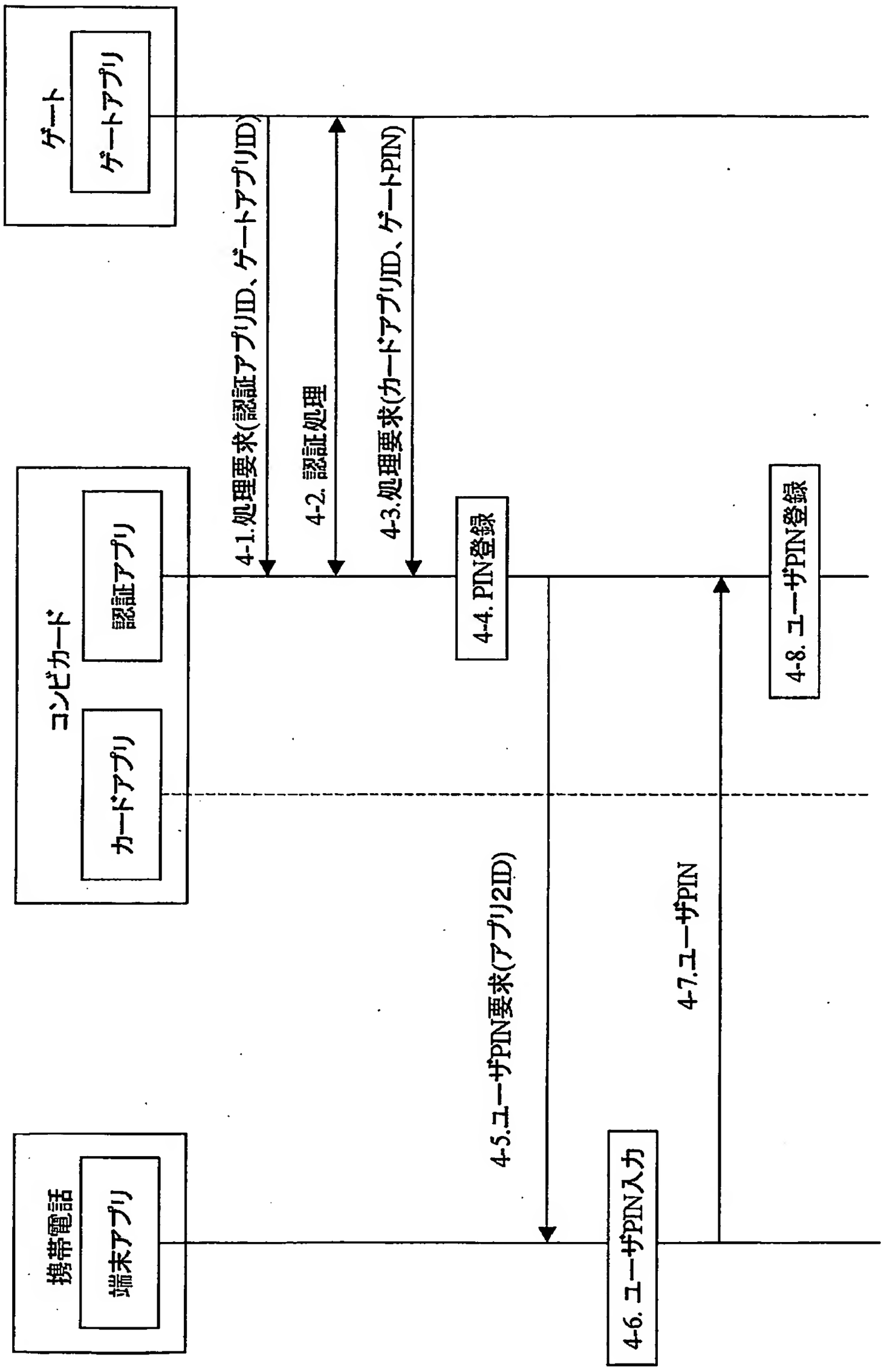
【図１４】


機器1
10
携帯電話
接触通信手段1
11
CPU
12
端末アプリ
14
機器2
20
コンビカード
接触通信手段2
21
非接触通信手段3
22
CPU
23
カードアプリ
29
認証アプリ
24
認証情報DB
25
PINDB
29
機器3
40
ゲート
非接触通信手段4
41
CPU
42
ゲートアプリ
43
機器4
50
金庫
非接触通信手段5
51
CPU
52
鍵アプリ
53

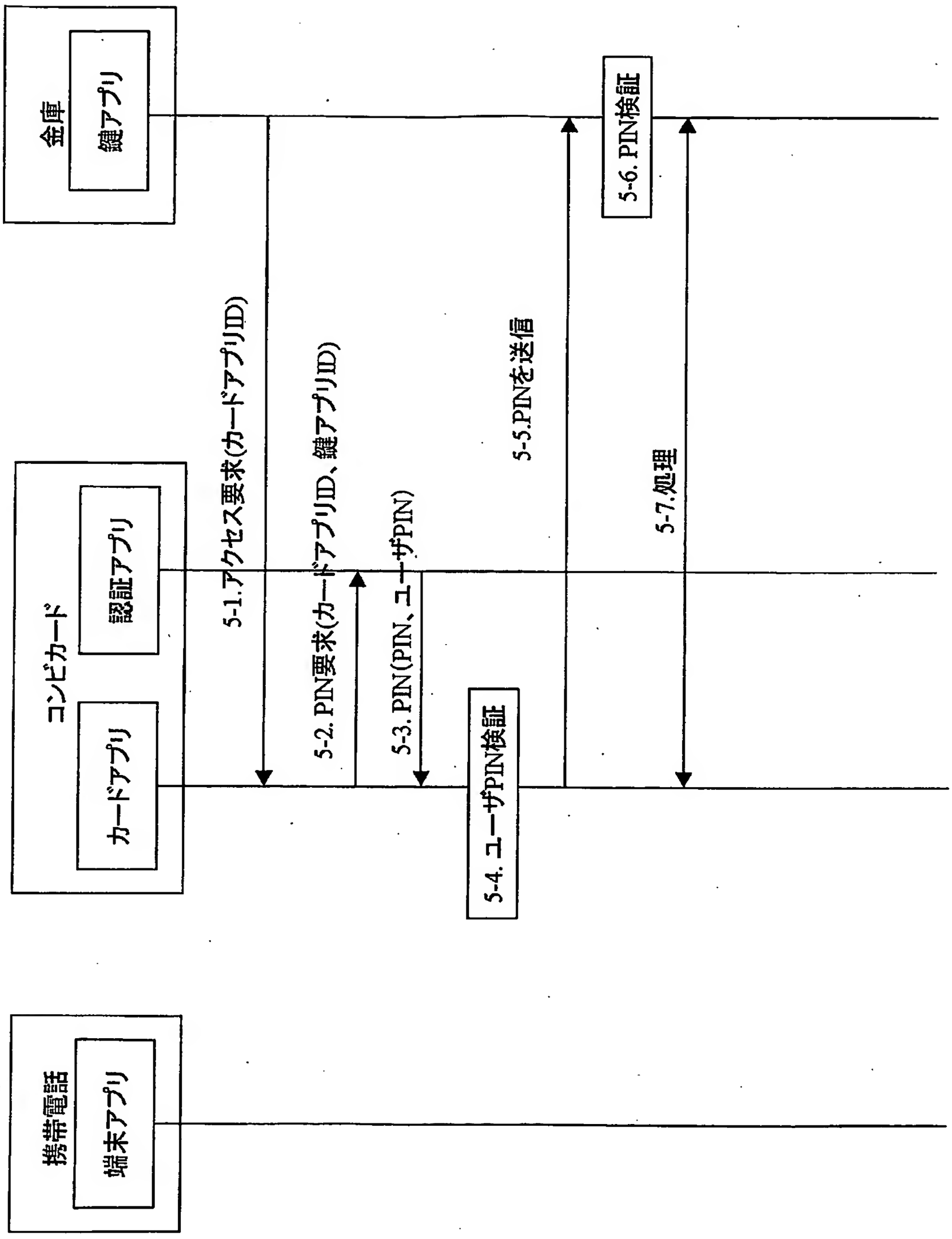
【図１５】


金庫
鍵アプリ
3-9. PIN検証
3-1.アクセス要求(カードアプリID)
3-2. PIN要求(カードアプリID、鍵アプリID)
3-3. ゲートPIN
3-8.PINを送信
3-10.処理
ユーザPIN要求
ユーザPIN
3-7. ユーザPIN検証
ユーザPIN入力
3-4.ユーザ
3-6.ユーザ
3-5. ユーザPIN入力
携帯電話
端末アプリ
認証アプリ
カードアプリ
ヨンピカード

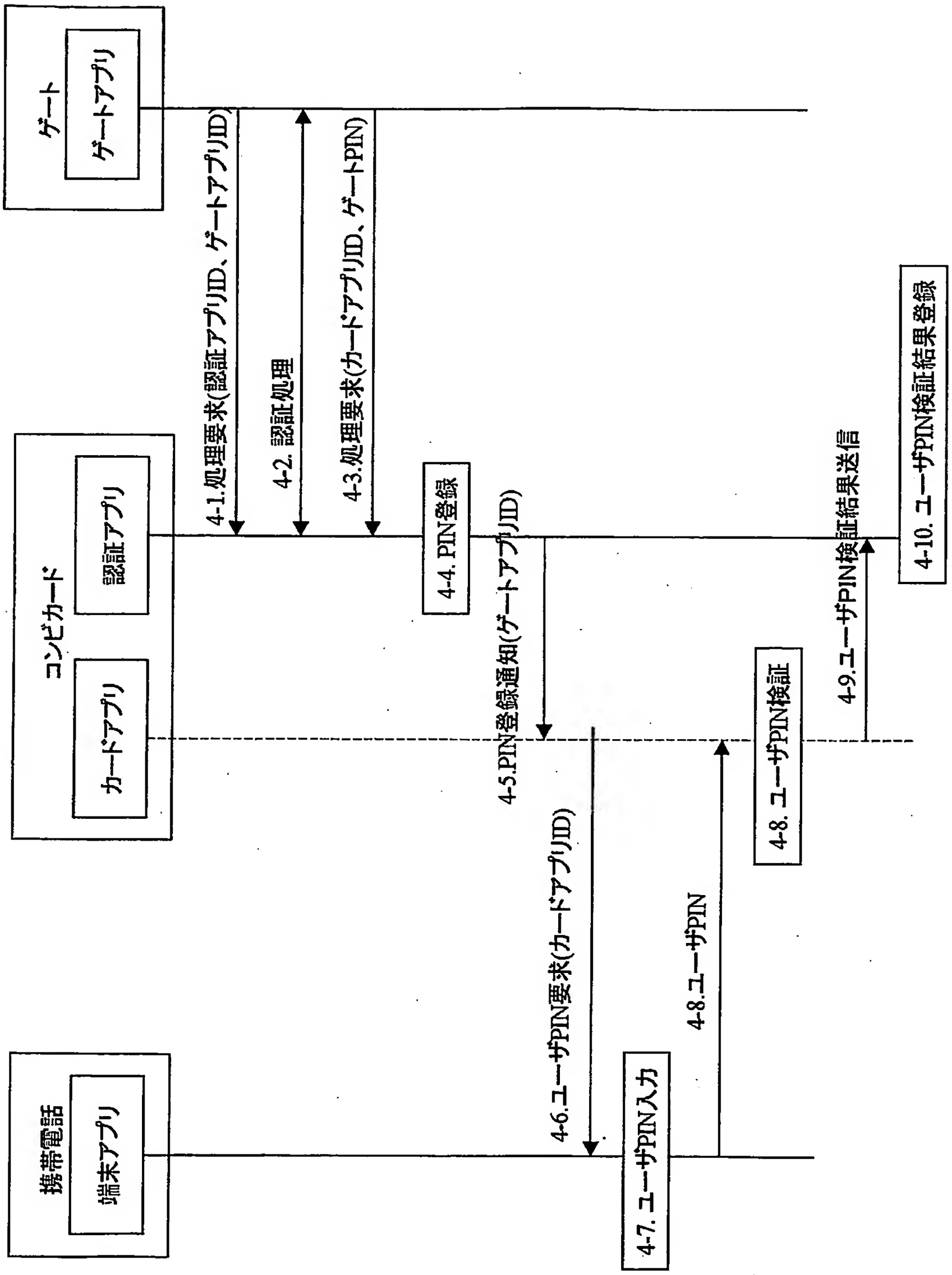
【図１６】


ゲート
ゲートアプリ
4-1.処理要求(認証アプリID、ゲートアプリID)
4-2. 認証処理
4-3.処理要求(カードアプリID、ゲートPIN)
ユンビカード
認証アプリ
カードアプリ
4-4. PIN登録
4-8. ユーザPIN登録
4-5.ユーザPIN要求(アプリ2ID)
4-7.ユーザPIN
携帯電話
端末アプリ
4-6. ユーザPIN入力

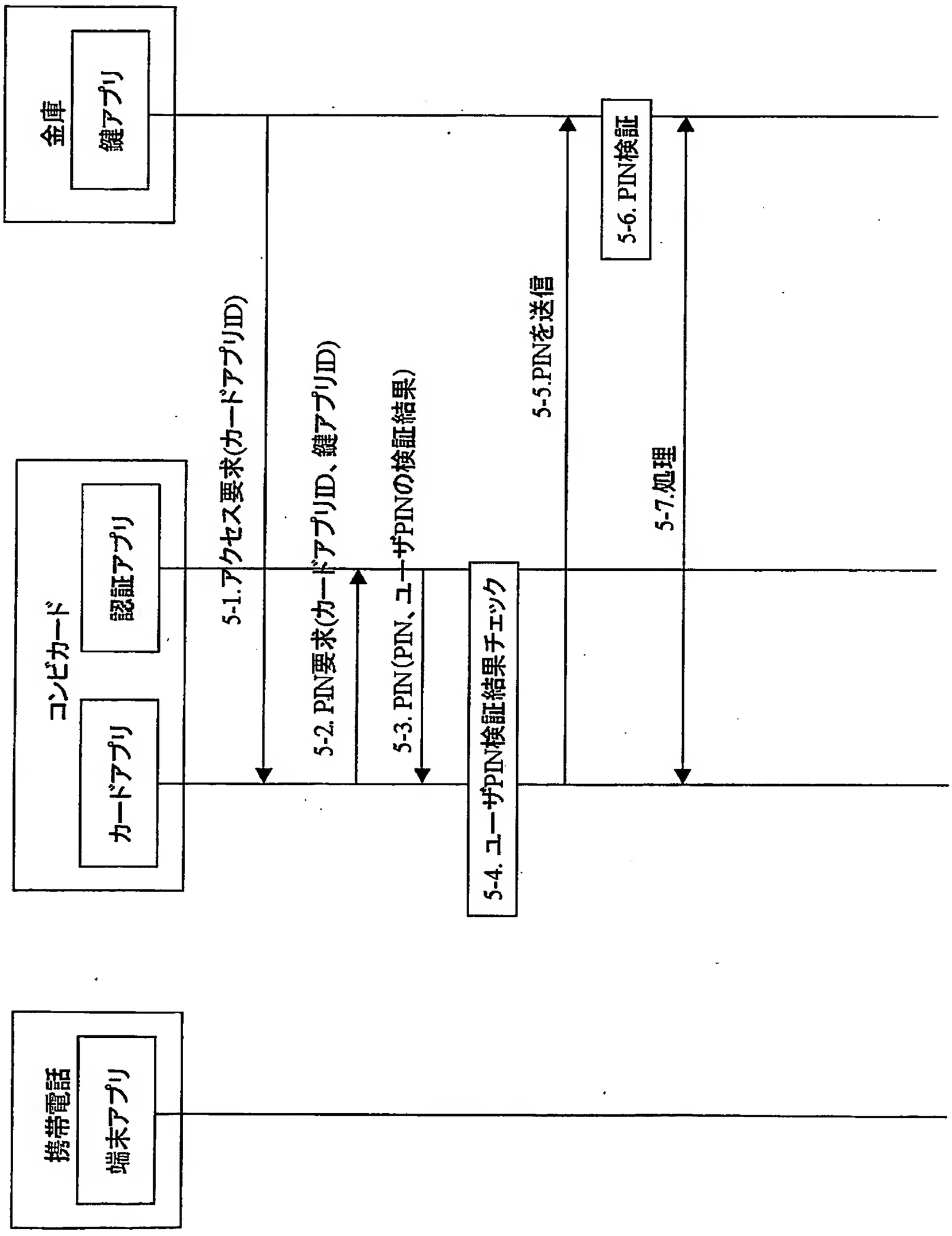
【図１７】


金庫
鍵アプリ
5-6. PIN検証
ユンビカード
認証アプリ
カードアプリ
5-1.アクセス要求(カードアプリID)
5-2. PIN要求(カードアプリID、鍵アプリID)
5-3. PIN(PIN、ユーザPIN)
5-4. ユーザPIN検証
5-5.PINを送信
5-7.処理
携帯電話
端末アプリ

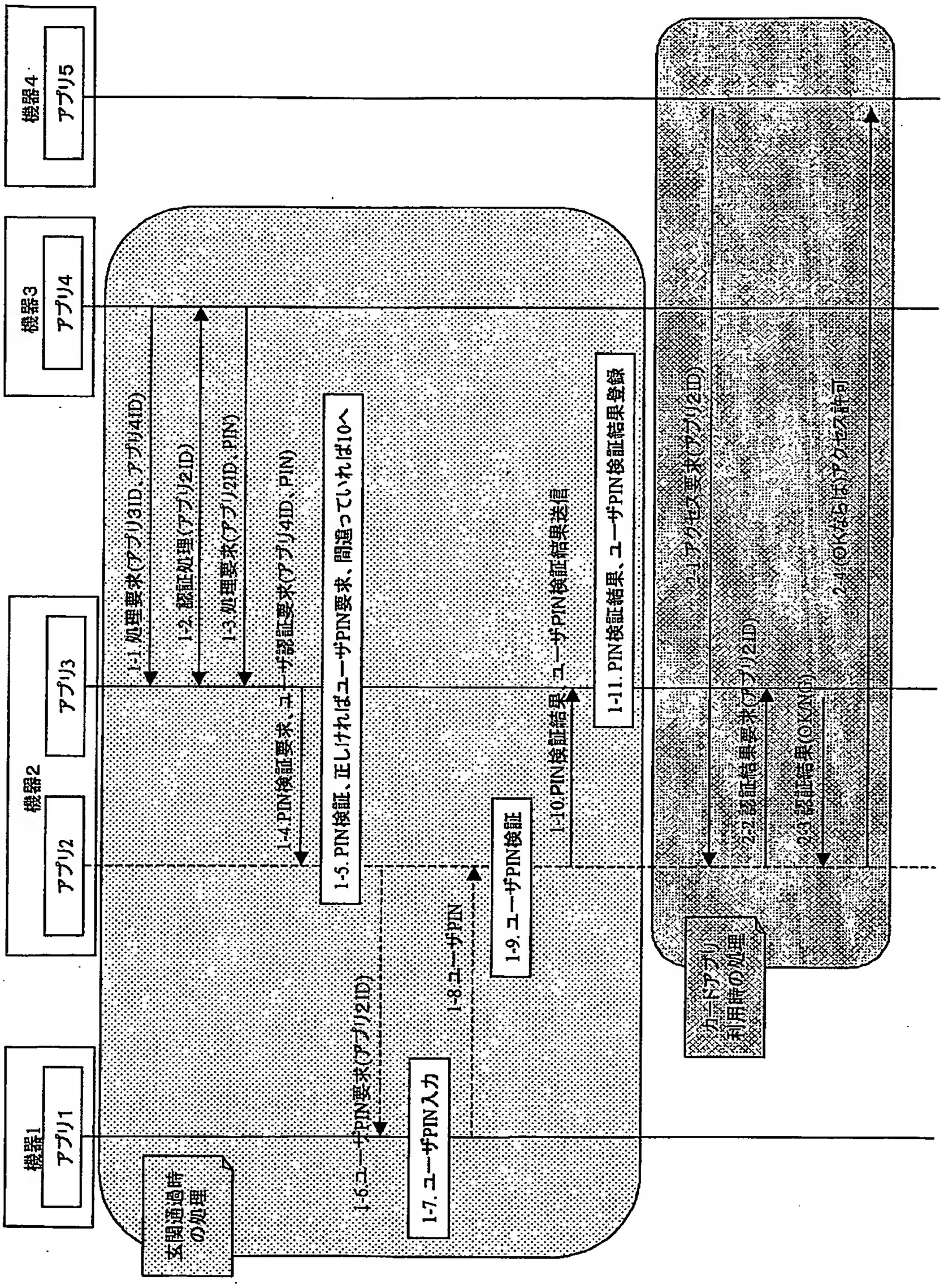
【図１８】


ゲート
ゲートアプリ
4-1.処理要求(認証アプリID、ゲートアプリID)
4-2. 認証処理
4-3.処理要求(カードアプリID、ゲートPIN)
4-4. PIN登録
4-5.PIN登録通知(ゲートアプリID)
4-6.ユーザPIN要求(カードアプリID)
4-7. ユーザPIN入力
4-8.ユーザPIN
4-8. ユーザPIN検証
4-9.ユーザPIN検証結果送信
4-10. ユーザPIN検証結果登録
コンビカード
認証アプリ
カードアプリ
携帯電話
端末アプリ

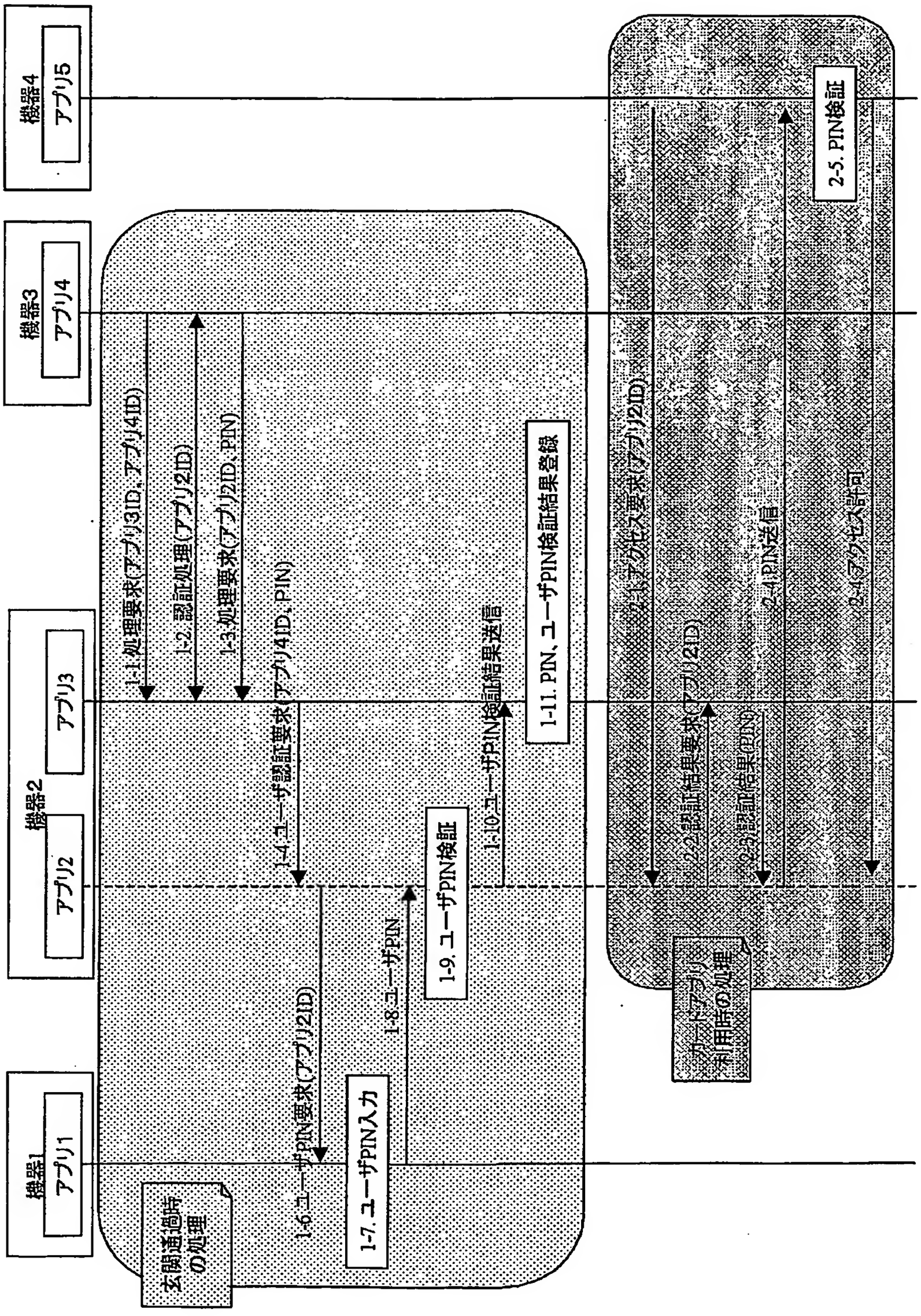
【図１９】


金庫
鍵アプリ
携帯電話
端末アプリ
コンビカード
カードアプリ
認証アプリ
5-1.アクセス要求(カードアプリID)
5-2. PIN要求(カードアプリID、鍵アプリID)
5-3. PIN(PIN、ユーザPINの検証結果)
5-4. ユーザPIN検証結果チェック
5-5.PINを送信
5-6. PIN検証
5-7.処理

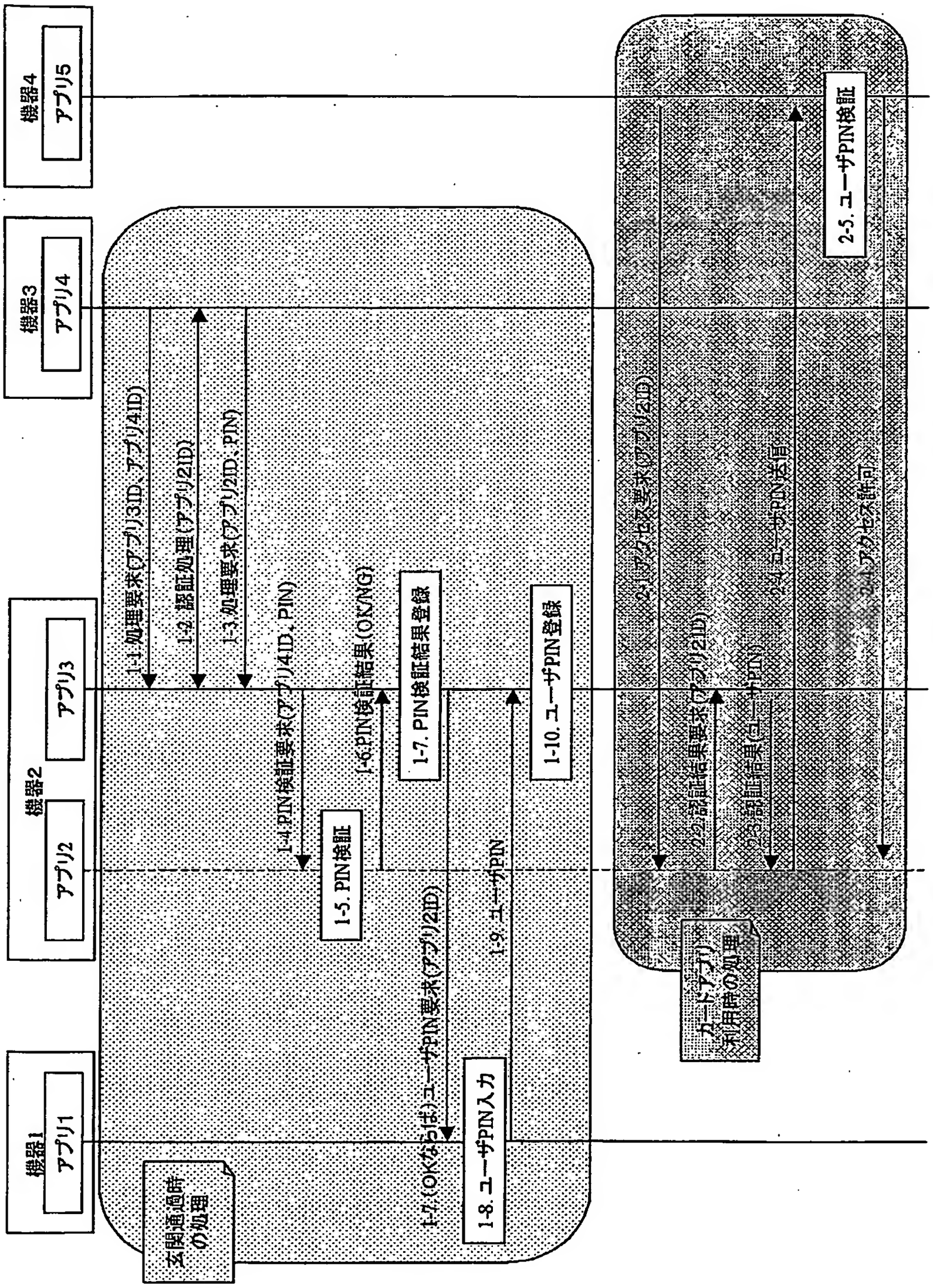
【図２０】


機器4
アプリ5
機器3
アプリ4
機器2
アプリ3
アプリ2
機器1
アプリ1
1-1.処理要求(アプリ3ID、アプリ4ID)
1-2.認証処理(アプリ2ID)
1-3.処理要求(アプリ2ID、PIN)
1-4.PIN検証要求、ユーザ認証要求(アプリ4ID、PIN)
1-5.PIN検証、正しければユーザPIN要求、間違っていれば10へ
1-6.ユーザPIN要求(アプリ2ID)
1-7.ユーザPIN入力
1-8.ユーザPIN
1-9.ユーザPIN検証
1-10.PIN検証結果、ユーザPIN検証結果送信
1-11.PIN検証結果、ユーザPIN検証結果登録
2-1.アクセス要求(アプリ2ID)
2-2.認証結果要求(アプリ2ID)
2-3.認証結果(OK/NG)
2-4.(OKなら)アクセス許可
玄関通過時の処理
カードアプリ利用時の処理

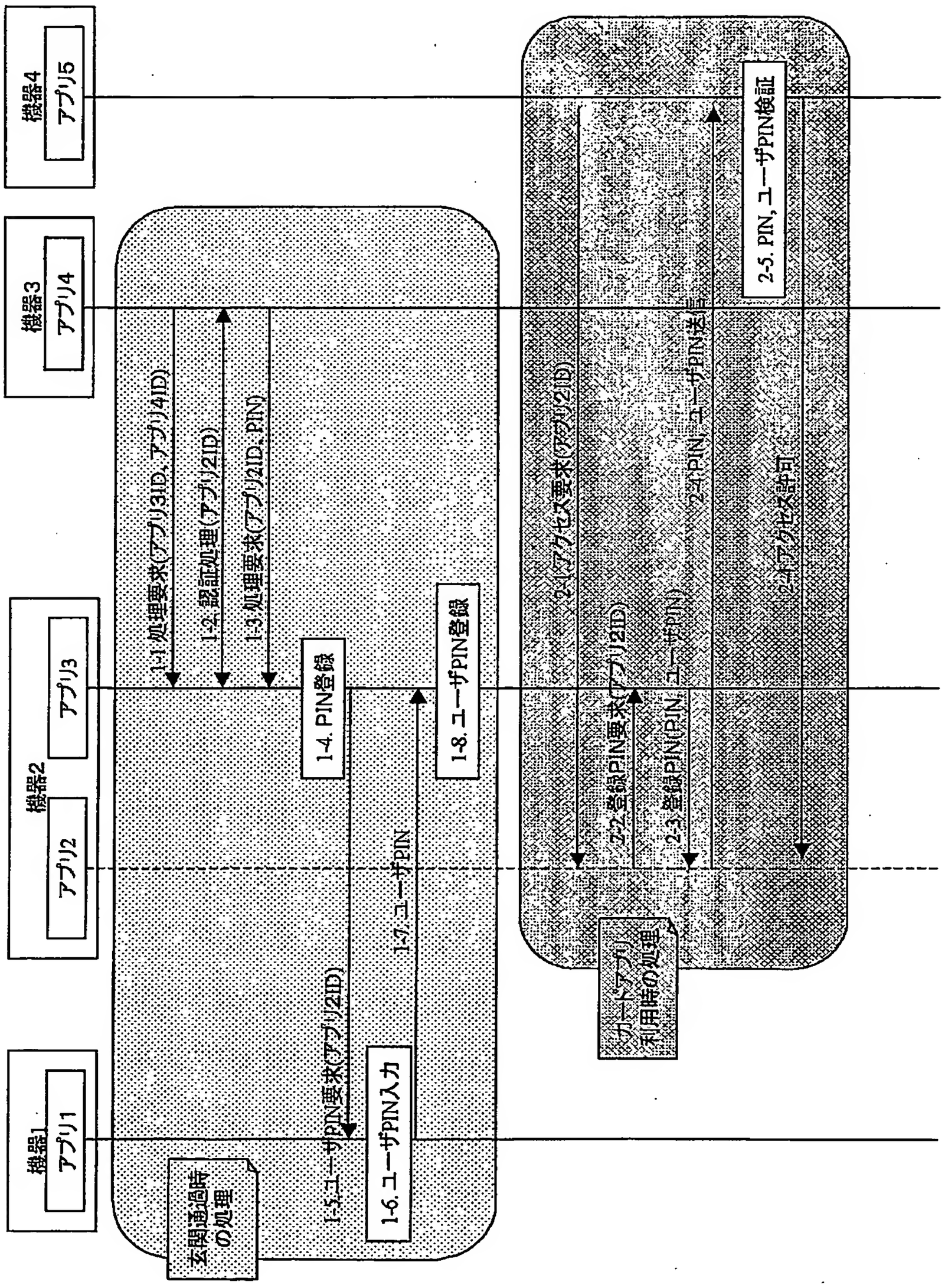
【図２１】


機器4
アプリ5
2-5. PIN検証
機器3
アプリ4
1-1.処理要求(アプリ3ID、アプリ4ID)
1-2.認証処理(アプリ2ID)
1-3.処理要求(アプリ2ID、PIN)
機器2
アプリ2
アプリ3
1-4.ユーザ認証要求(アプリ4ID、PIN)
1-10.ユーザPIN検証結果送信
1-11. PIN、ユーザPIN検証結果登録
2-1.アクセス要求(アプリ2ID)
2-2.認証結果要求(アプリ2ID)
2-3.認証結果(PIN)
2-4.PIN送信
2-6.アクセス許可
1-8.ユーザPIN
1-9.ユーザPIN検証
1-6.ユーザPIN要求(アプリ2ID)
1-7.ユーザPIN入力
機器1
アプリ1
公開通過時の処理
カードアプリ利用時の処理

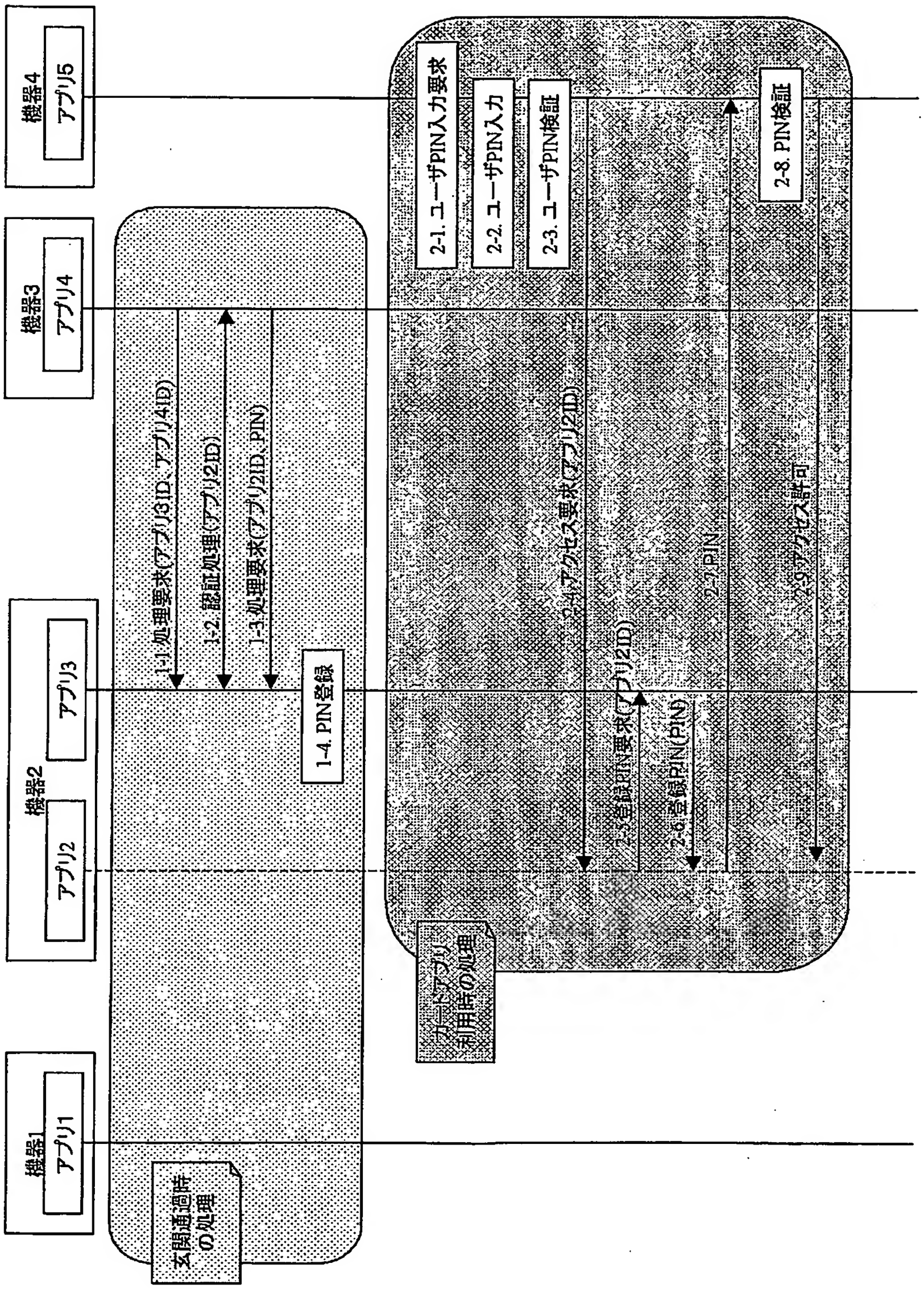
【図２２】


機器4
アプリ5
機器3
アプリ4
機器2
アプリ2
アプリ3
機器1
アプリ1
1-1.処理要求(アプリ3ID、アプリ4ID)
1-2.認証処理(アプリ2ID)
1-3.処理要求(アプリ2ID、PIN)
1-4.PIN検証要求(アプリ4ID、PIN)
1-5.PIN検証
1-6.PIN検証結果(OK/NG)
1-7.PIN検証結果登録
1-8.ユーザPIN入力
1-9.ユーザPIN要求(アプリ2ID)
1-10.ユーザPIN登録
2-1.アクセス要求(アプリ2ID)
2-2.認証結果要求(アプリ2ID)
2-3.認証結果(ユーザPIN)
2-4.ユーザPIN送信
2-5.ユーザPIN検証
2-6.アクセス許可
カードアプリ利用時の処理
玄関通過時の処理

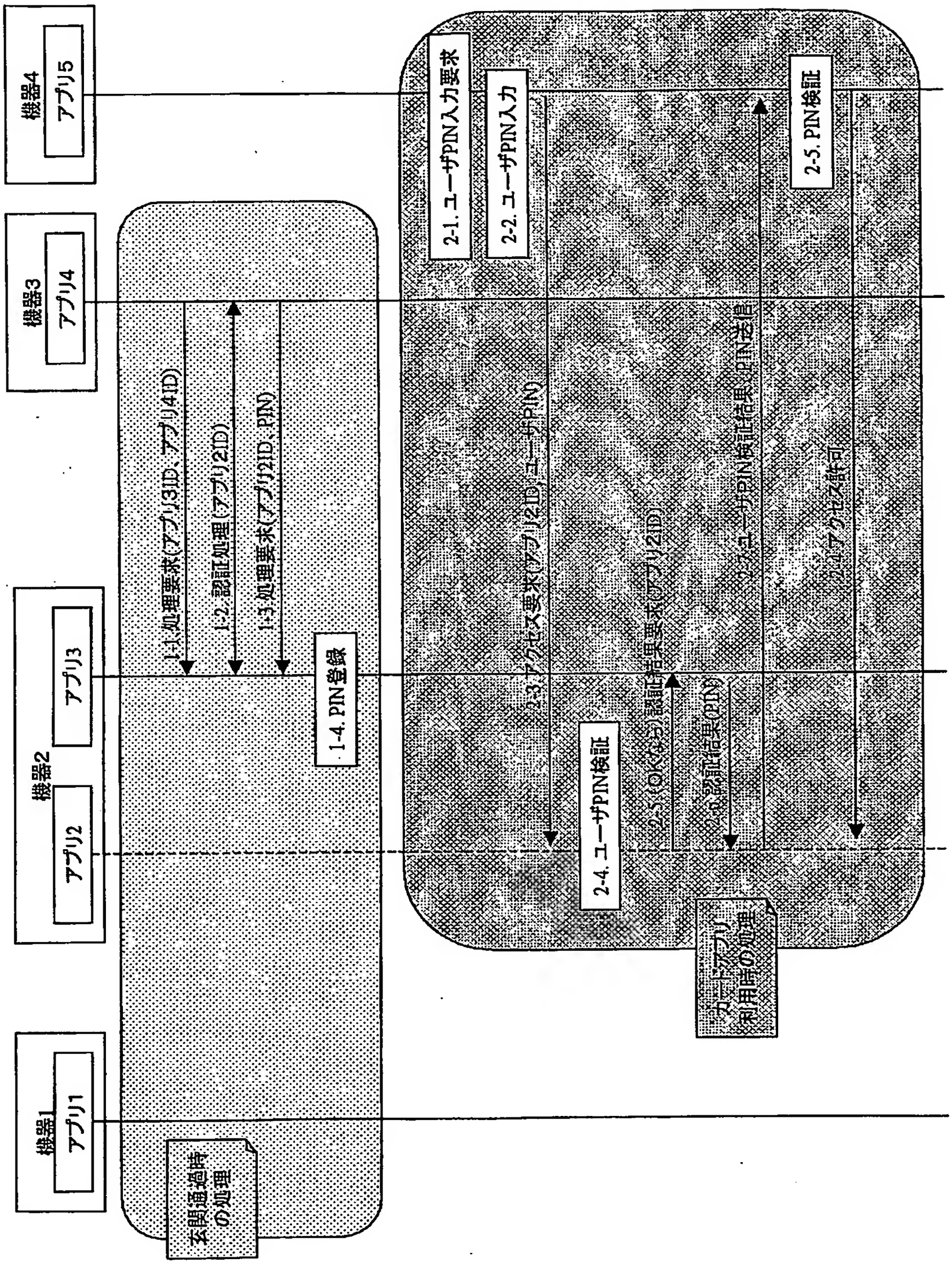
【図２３】


機器4
アプリ5
機器3
アプリ4
機器2
アプリ2
アプリ3
機器1
アプリ1
1-1.処理要求(アプリ3ID, アプリ4ID)
1-2.認証処理(アプリ2ID)
1-3.処理要求(アプリ2ID, PIN)
1-4.PIN登録
1-5.ユーザPIN要求(アプリ2ID)
1-6.ユーザPIN入力
1-7.ユーザPIN
1-8.ユーザPIN登録
2-1.アクセス要求(アプリ2ID)
2-2.登録PIN要求(アプリ2ID)
2-3.登録PIN(PIN, ユーザPIN)
2-4.PIN, ユーザPIN送信
2-5.PIN, ユーザPIN検証
2-6.アクセス許可
玄関通過時の処理
ゲートアプリ利用時の処理

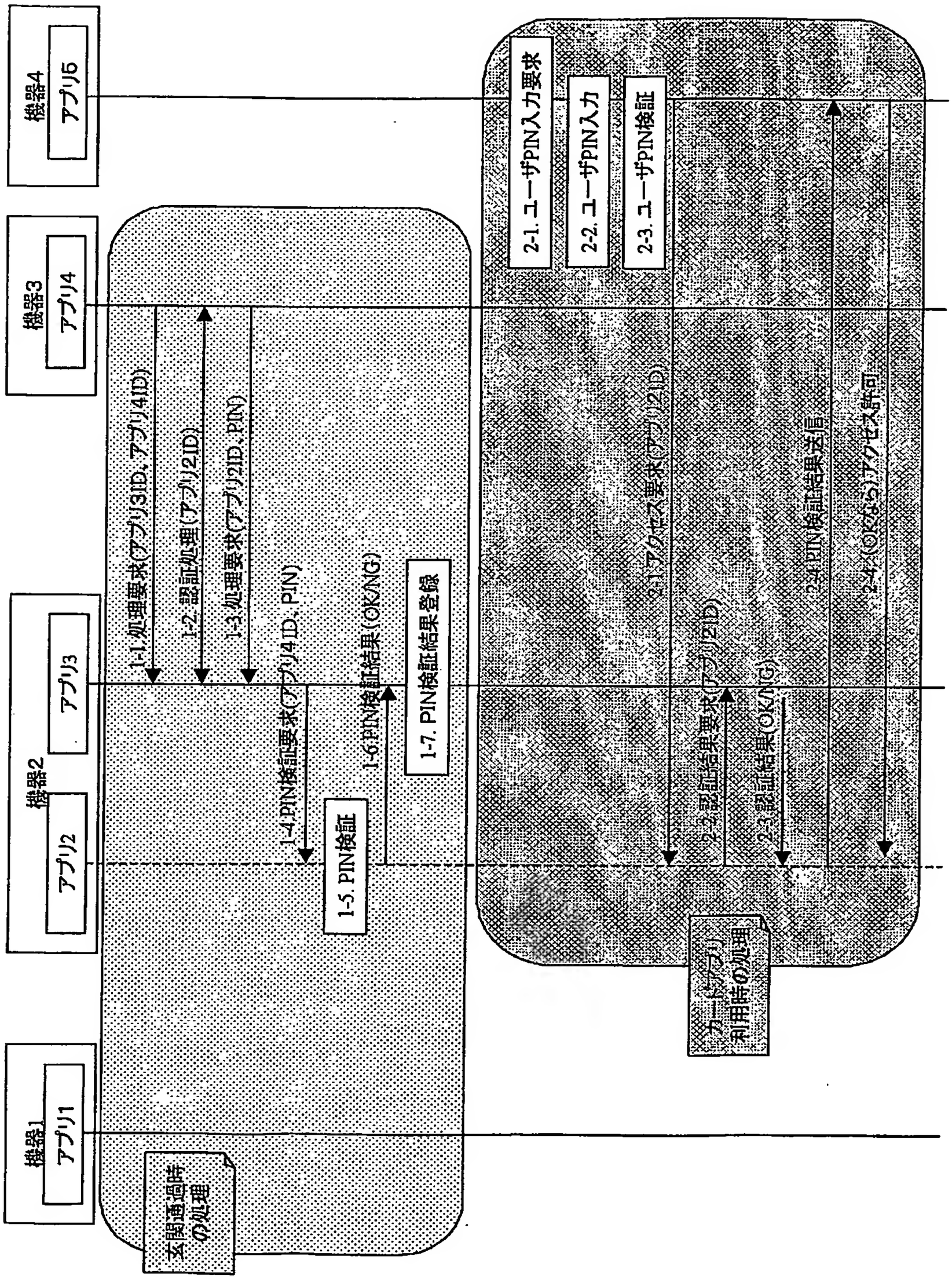
【図２４】


機器4
アプリ5
機器3
アプリ4
機器2
アプリ2
アプリ3
機器1
アプリ1
1-1 処理要求(アプリ3ID、アプリ4ID)
1-2 認証処理(アプリ2ID)
1-3 処理要求(アプリ2ID、PIN)
1-4 PIN登録
玄関通過時の処理
2-1 ユーザPIN入力要求
2-2 ユーザPIN入力
2-3 ユーザPIN検証
2-4 ユーザアクセス要求(アプリ2ID)
2-5 登録PIN要求(アプリ2ID)
2-6 登録PIN(PIN)
2-7 PIN
2-8 PIN検証
2-9 アクセス許可
カードアプリ利用時の処理

【図２５】


機器4
アプリ5
機器3
アプリ4
機器2
アプリ2
アプリ3
機器1
アプリ1
1-1.処理要求(アプリ3ID、アプリ4ID)
1-2.認証処理(アプリ2ID)
1-3.処理要求(アプリ2ID、PIN)
1-4. PIN登録
玄関通過時の処理
2-1.ユーザPIN入力要求
2-2.ユーザPIN入力
2-3.アクセス要求(アプリ2ID、ユーザPIN)
2-4.ユーザPIN検証
2-5.(OKなら)認証結果要求(アプリ2ID)
2-6.認証結果(PIN)
2-7.ユーザPIN検証結果、PIN送信
2-8.アクセス許可
2-4. ユーザPIN検証
ドアアプリ利用時の処理

【図２６】


機器4
アプリ5
機器3
アプリ4
機器2
アプリ2
アプリ3
機器1
アプリ1
2-1.ユーザPIN入力要求
2-2.ユーザPIN入力
2-3.ユーザPIN検証
1-1.処理要求(アプリ3ID, アプリ4ID)
1-2.認証処理(アプリ2ID)
1-3.処理要求(アプリ2ID, PIN)
1-4.PIN検証要求(アプリ4ID, PIN)
1-5.PIN検証
1-6.PIN検証結果(OK/NG)
1-7. PIN検証結果登録
2-1.アクセス要求(アプリ2ID)
2-2.認証結果要求(アプリ2ID)
2-3.認証結果(OK/NG)
2-4.PIN検証結果送信
2-4:(OKなら)アクセス許可
玄関通過時の処理
カード利用時の処理

【書類名】要約書
【要約】
【課題】カードアプリ機能や装置機能等が発現されるエリアを限定できるＩＣカード等のセキュアデバイスを提供する。
【解決手段】セキュアデバイス２０に、ゲート機器４０に対して認証処理を行う認証手段２４と、端末１０にインストールする端末アプリ２６、２７と、認証手段２４がゲート機器４０との認証に成功した場合に、ゲート機器４０から指定された端末アプリを端末１０にインストールする制御手段２３とを設けている。セキュアデバイス２０をゲート機器４０に翳し、正常に通過したエリアでのみ、端末アプリ２６、２７が端末１０にインストールされる。ゲート機器４０のゲートアプリ４３が特定の領域で機能するアプリを指定するので、ユーザの登録操作等は不要であり、また、端末へのＧＰＳ受信機等の装備も必要がない。
【選択図】図１

特願２００４－０１９４６１

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

出証番号　出証特２００５－３０１９９８６